(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 400 398**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/10 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.03.2008 E 08400015 (7)**

(97) Fecha y número de publicación de la concesión europea: **26.12.2012 EP 2106191**

(54) Título: **Procedimiento para actualizar una tarjeta inteligente y tarjeta inteligente con capacidad de actualización**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.04.2013

(73) Titular/es:

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

(72) Inventor/es:

KORAICHI, NAJIB y
MONTANER, JAVIER

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento para actualizar una tarjeta inteligente y tarjeta inteligente con capacidad de actualización

Campo técnico

La invención se refiere a la administración de una tarjeta inteligente conectada con un terminal móvil que tiene acceso a una red de comunicación móvil. En particular, la invención se refiere a la transmisión de datos a la tarjeta inteligente. La tarjeta inteligente puede ser un módulo de identificación de usuario, que es utilizado específicamente para identificar y autenticar a un usuario móvil ante la red de comunicación móvil.

Trasfondo de la invención

Las tarjetas inteligentes son tarjetas que contienen un circuito integrado incrustado para procesar información. El circuito incrustado comprende una memoria para almacenar datos y puede comprender adicionalmente un componente de microprocesador para ejecutar aplicaciones y manipular datos. En los sistemas de comunicación móvil, tales tarjetas inteligentes son usadas como módulos de identificación de usuario, que identifican específicamente y autentican a un usuario móvil ante una red de comunicación móvil. Además, tales tarjetas inteligentes son usadas para proporcionar servicios adicionales en el sistema de comunicación móvil, para almacenar datos personales del usuario móvil y para almacenar datos de configuración del dispositivo de comunicación móvil, por ejemplo. En el GSM (Sistema Global para la comunicación Móvil), las tarjetas inteligentes están configuradas como un SIM (Módulo de Identidad de Abonado). En el UMTS (Sistema Universal para la Telecomunicación Móvil), las tarjetas inteligentes están configuradas como una UICC (Tarjeta de Circuitos Integrados de USIM), que comprende una aplicación USIM (Módulo de Identidad Universal de Abonado). Las tarjetas inteligentes están bajo control del operador de red móvil que emitió las tarjetas. Esto significa que los datos y aplicaciones sensibles solamente pueden ser modificados con el permiso del operador de red móvil.

La denominada tecnología por el aire (OTA), según se describe, por ejemplo, en los documentos ETSI TS 102 225 y 3GPP TS 23.048, permite actualizar o cambiar datos y / o aplicaciones en la tarjeta inteligente sin tener que re-emitir la tarjeta. La tecnología OTA usa una arquitectura de cliente / usuario, donde en un extremo hay un sistema de trastienda y en el otro extremo está la tarjeta inteligente. El sistema de trastienda comprende una base de datos que proporciona los datos y una pasarela OTA, que está habitualmente operada por el operador de red móvil, y que envía los datos a la tarjeta inteligente mediante la red de comunicación móvil. La pasarela OTA cifra los datos usando una clave, que está compartida entre la pasarela OTA y la tarjeta inteligente. La tarjeta inteligente descifra los datos usando una correspondiente clave de descifrado, confirmando por ello que los datos se originan en el operador de red móvil. Si los datos no pueden ser validados con éxito, la tarjeta inteligente deniega el acceso a su memoria y a otras funciones, y los datos no pueden ser almacenados en la tarjeta inteligente.

En los entornos OTA de hoy, se usa usualmente el SMS (Servicio de Mensajes Breves) para transmitir los datos a la tarjeta inteligente. En particular, cuando tienen que descargarse aplicaciones nuevas o actualizadas en la tarjeta inteligente, la cantidad de datos usualmente supera el tamaño de un mensaje breve, y los datos son distribuidos entre varios mensajes breves, que son enviados a la tarjeta inteligente. En consecuencia, la descarga de una mayor cantidad de datos en la tarjeta inteligente, tal como, por ejemplo, una aplicación nueva o actualizada, impone una carga relativamente enorme a la pasarela OTA y a la red de comunicación móvil, dado que los datos tienen que ser enviados desde la pasarela OTA a la tarjeta inteligente mediante la red de comunicación móvil.

El documento WO 2008 / 035183 revela un procedimiento para transferir datos desde un servidor a una estación móvil, usando un mecanismo OTA. El servidor envía primero una notificación a la estación móvil, informando por ello a la estación móvil de que hay datos por transferir a la estación móvil. Cuando la estación móvil recibe la notificación, genera una clave de transporte y envía una solicitud que incluye una clave de transporte al servidor. La clave de transporte es cifrada usando una clave de sesión proporcionada por el servidor en la notificación. Cuando el servidor recibe la solicitud, usa la clave de transporte para cifrar los datos, para su transferencia a la estación móvil.

El documento EP 0 798 673 describe un procedimiento para cargar comandos con seguridad en una tarjeta inteligente. Los comandos son proporcionados por un primer participante y son transferidos junto con códigos de autenticación producidos por participantes adicionales. La tarjeta reproduce los códigos de autenticación usando las correspondientes claves y compara los códigos reproducidos con los códigos transferidos, a fin de validar los comandos. Las claves están pre-instaladas en la tarjeta.

El documento WO 01 / 58081 A1 describe un procedimiento para comprobar la integridad de los datos. En el mensaje, un mensaje es transmitido a un dispositivo de comunicación móvil a través de un primer canal, y un código de comprobación es enviado al dispositivo de comunicación móvil a través de un segundo canal. El dispositivo de comunicación móvil usa el código de comprobación para verificar la integridad del mensaje.

Resumen de la invención

Es un objeto de la presente invención reducir la carga de la pasarela OTA que contiene la clave de cifrado para la comunicación segura, al descargar datos en una tarjeta inteligente usando un mecanismo OTA.

El objeto es logrado por un procedimiento que comprende las características de la reivindicación 1 y por una tarjeta que comprende las características de la reivindicación 10. Las realizaciones del procedimiento y de la tarjeta inteligente se dan en las reivindicaciones dependientes.

La invención implica la idea de dividir la descarga de los datos y de un testigo de seguridad para validar los datos entre dos etapas. Esto tiene la ventaja de que el testigo de seguridad puede ser proporcionado en una etapa de transmisión que sea independiente de la transmisión de los datos a la tarjeta inteligente. Esto lleva a la ventaja adicional de que los datos no tienen que ser proporcionados por el servidor que proporciona el testigo de seguridad, reduciendo por ello la carga de este servidor. Dado que el testigo de seguridad comprende una característica de seguridad y no los mismos datos a descargar, tiene un volumen de datos más pequeño que los datos a descargar. Los datos son proporcionados por una base de datos que puede estar conectada con el terminal móvil.

La tarjeta inteligente puede comprender un módulo de identificación de usuario, en particular, un SIM y / o un USIM. Sin embargo, la tarjeta inteligente podría ser cualquier tarjeta inteligente conectada con un terminal móvil.

La conexión entre el servidor y la tarjeta inteligente está establecida mediante el terminal móvil. Cuando el terminal móvil recibe el testigo de seguridad, remite el testigo de seguridad a la tarjeta inteligente, donde es recibido en el componente receptor.

En una realización del procedimiento y de la tarjeta inteligente, la parte cifrada del testigo de seguridad está cifrada usando una clave de cifrado almacenada con seguridad en el servidor, y la parte cifrada del testigo de seguridad es descifrada usando una clave de descifrado adjudicada a la clave de cifrado, estando la clave de descifrado almacenada con seguridad en la tarjeta inteligente.

Dado que el cifrado se hace usando una clave almacenada con seguridad en el servidor, la autenticidad del testigo de seguridad puede ser comprobada descifrando las partes cifradas del testigo de seguridad. En particular, el testigo de seguridad se origina en el servidor solamente si su parte cifrada puede ser descifrada usando la clave de descifrado adjudicada a la clave de cifrado usada en el servidor.

En una realización del procedimiento y de la tarjeta inteligente, la característica de seguridad comprende una suma de control de los datos, siendo usada la suma de control en la tarjeta inteligente para validar la integridad de los datos.

La suma de control es una información obtenida de manera única a partir de los datos, tal como, por ejemplo, una función de troceo calculada usando un algoritmo de troceo conocido por una persona experta en la técnica. Dado que la suma de control es distinta, cuando los datos son modificados, la suma de control permite validar la integridad de los datos. Esto significa que se comprueba que los datos no hayan sido modificados sin permiso. La suma de control puede ser proporcionada al servidor por la base de datos antes de enviar el testigo de seguridad al terminal móvil y / o a la tarjeta inteligente.

En una realización adicional del procedimiento y de la tarjeta inteligente, la tarjeta inteligente extrae los datos de la base de datos en respuesta a la recepción del testigo de seguridad, usando información contenida en el testigo de seguridad.

Ventajosamente, en esta realización, la tarjeta inteligente recibe el testigo de seguridad al principio. Luego, la tarjeta inteligente usa la información contenida en el testigo de seguridad para extraer los datos de la base de datos. Esta información puede comprender información que identifica los datos y / o información para abordar la base de datos.

En una realización adicional del procedimiento y de la tarjeta inteligente, el servidor envía un comando a la base de datos con respecto a la transmisión del testigo de seguridad a la tarjeta inteligente, instruyendo el comando a la base de datos para transmitir los datos a la tarjeta inteligente.

En esta realización, la transmisión de los datos a la tarjeta inteligente es iniciada por el servidor con relación a la transmisión del testigo de seguridad a la tarjeta inteligente. En particular, el servidor puede iniciar la transmisión de los datos a la tarjeta inteligente después de haber enviado el testigo de seguridad a la tarjeta inteligente. El comando para instruir a la base de datos para transmitir los datos a la tarjeta inteligente puede comprender información que identifica los datos y / o información que identifica a la tarjeta inteligente.

Una realización del procedimiento y de la tarjeta inteligente provee que los datos estén cifrados, y en la cual la tarjeta inteligente descifra los datos usando una clave de descifrado contenida en el testigo de seguridad.

Esta realización mejora el nivel de seguridad proporcionando los datos en forma cifrada. En particular, esto impide que

terceros vean los datos mientras son transmitidos a la tarjeta inteligente. Ventajosamente, la clave usada para descifrar los datos en la tarjeta inteligente es proporcionada en el testigo de seguridad. Dentro del testigo de seguridad, esta clave puede estar contenida en la parte cifrada, de modo que esté protegida contra el acceso por terceros no autorizados.

En una realización del procedimiento y de la tarjeta inteligente, la tarjeta inteligente está conectada con la base de datos mediante el terminal móvil, estando el terminal móvil conectado con la base de datos mediante la red de comunicación móvil, o una red de datos.

En esta realización, una conexión entre la tarjeta inteligente y la base de datos es establecida por el terminal móvil. El terminal móvil está conectado con la base de datos mediante la red de comunicación móvil o mediante otra red de datos, tal como, por ejemplo, Internet. Cuando son recibidos en el terminal móvil, el terminal móvil pasa los datos a la tarjeta inteligente.

Una realización adicional del procedimiento y de la tarjeta inteligente provee que el primer canal de comunicación y / o el segundo canal de comunicación sea un canal de SMS.

Ventajosamente, en esta realización, el SMS es usado para transmitir el testigo de seguridad a la tarjeta inteligente y / o para transmitir los datos a la tarjeta inteligente. Preferiblemente, los mensajes de SMS son recibidos en el terminal móvil, que remite los mensajes a la tarjeta inteligente conectada con el terminal móvil. En particular, el SMS puede ser usado para transmitir los datos a la tarjeta inteligente, si el terminal móvil y la base de datos están conectados entre sí mediante la red de comunicación móvil.

Sin embargo, los datos pueden ser transmitidos a la tarjeta inteligente mediante un canal de comunicación que sea distinto al canal de comunicación mediante el cual es transmitido el testigo de seguridad a la tarjeta inteligente. Por lo tanto, en una realización del procedimiento y de la tarjeta inteligente, el segundo canal de comunicación es distinto al primer canal de comunicación.

Esto permite una mayor flexibilidad al escoger el canal de comunicación para transmitir los datos a la tarjeta inteligente. En general, el testigo de seguridad tiene un volumen de datos mucho más pequeño que los datos en sí. Por tanto, el segundo canal de comunicación para transmitir los datos a la tarjeta inteligente puede ser un canal de comunicación que proporcione altas velocidades de transferencia de datos. En particular, el segundo canal de comunicación puede ser un canal del GPRS (GPRS: Servicio General de Radio por Paquetes) u otro canal de comunicación de datos proporcionado por la red que conecta el terminal móvil con la base de datos. Un ejemplo de un canal de comunicación de ese tipo es un canal de comunicación basado en el protocolo de Internet (IP). El primer canal de comunicación para transmitir el testigo de seguridad a la tarjeta inteligente puede ser escogido independientemente del segundo canal de comunicación. Debido al pequeño volumen de datos del testigo de seguridad, el segundo canal de comunicación puede ser un canal de comunicación que tenga una menor velocidad de transferencia de datos.

En una realización del procedimiento y de la tarjeta inteligente, la base de datos está contenida en un módulo adaptador, que es conectable con la tarjeta inteligente.

En una realización relacionada del procedimiento y de la tarjeta inteligente, el módulo adaptador está conectado entre el terminal móvil y la tarjeta inteligente.

Las realizaciones precitadas tienen la ventaja de que los datos son proporcionados por un módulo adaptador que puede ser conectado directamente con la tarjeta inteligente. En particular, el módulo adaptador puede estar conectado entre el terminal móvil y la tarjeta inteligente. En estas realizaciones, no es necesario descargar los datos en la tarjeta inteligente a través de una red de datos. Sin embargo, la autenticidad y la integridad de los datos están garantizadas por medio del testigo de seguridad proporcionado por el servidor para validar los datos. Aunque el módulo adaptador es conectable directamente con la tarjeta inteligente, el uso de los datos proporcionados por el módulo adaptador está aprobado por el servidor y por medio del testigo de seguridad.

Además, en una realización del procedimiento y de la tarjeta inteligente, los datos son proporcionados en una pantalla conectada con la base de datos, y adquiridos por medio de un sensor con cámara proporcionado por el terminal móvil, y en donde el terminal móvil pasa los datos adquiridos a la tarjeta inteligente.

En esta realización, el terminal móvil comprende un sensor con cámara para adquirir los datos, que son proporcionados en una pantalla. Esto también tiene la ventaja de que los datos no tienen que ser descargados en la tarjeta inteligente mediante una red de datos. Además, esta realización puede hacer uso del hecho de que los terminales móviles, tales como, por ejemplo, los teléfonos móviles o los PDA (Asistentes Personales de Datos), a menudo comprenden un sensor con cámara como una característica estándar.

En una realización adicional del procedimiento y de la tarjeta inteligente, los datos son proporcionados en una pantalla en forma codificada, en particular, como un código de barras.

Esta realización tiene la ventaja de que los datos codificados, especialmente los códigos de barras, pueden ser adquiridos electrónicamente con más facilidad. El código de barras puede ser un código de barras bidimensional o un código de barras tridimensional, por ejemplo.

Según un aspecto adicional de la invención, se proporciona un programa de ordenador. El programa de ordenador es cargable en la memoria interna de un ordenador digital y comprende partes de código de software para realizar las etapas de un procedimiento del tipo descrito anteriormente cuando el programa de ordenador es ejecutado en un ordenador.

Según un aspecto adicional de la invención, se proporciona un sistema. El sistema comprende una tarjeta inteligente del tipo descrito anteriormente. Además, el sistema comprende un servidor conectado con la red de comunicación móvil, para transmitir el testigo de seguridad a la tarjeta inteligente, y una base de datos conectable con la tarjeta inteligente, para transmitir los datos a la tarjeta inteligente.

Los precitados, y otros, aspectos de la invención, también serán evidentes a partir de, y aclarados con referencia a, las realizaciones descritas a continuación en la presente memoria, haciendo referencia a los dibujos.

Breve descripción de los dibujos

En los dibujos adjuntos

la Fig. 1 es una ilustración esquemática de un sistema de comunicación que comprende una tarjeta inteligente en la cual los datos pueden ser descargados,

la Fig. 2 es un diagrama de bloques esquemático que ilustra componentes de la tarjeta inteligente usados en el proceso de descarga de datos,

la Fig. 3 es un diagrama de flujo esquemático que ilustra procesos de descarga de datos en la tarjeta inteligente, y

la Fig. 4 es un diagrama de bloques esquemático que ilustra un módulo adaptador conectado entre un terminal móvil y una tarjeta inteligente.

Descripción detallada de realizaciones de la invención

La Fig. 1 ilustra esquemáticamente un sistema de comunicación móvil que comprende un terminal móvil 100, tal como, por ejemplo, un teléfono celular, un PDA (Asistente Personal de Datos) o similar, que está conectado inalámbricamente con una PLMN (Red Móvil Pública Terrestre) 102 mediante una red 104 de acceso por radio. La PLMN 102 es una red central del sistema de comunicación móvil operado por un operador de red móvil, y puede ser configurada según el estándar GSM, o según el estándar UMTS, por ejemplo. La red 104 de acceso por radio puede ser configurada como una GERAN (Red de Acceso por Radio EDGE del GSM), según el estándar de GSM, o como una UTRAN (Red de Acceso Universal Terrestre por Radio) según el estándar de UMTS, por ejemplo.

El terminal móvil 100 comprende una interfaz 115 de radio para conectar el terminal móvil 100 con la PLMN 102 mediante la red 104 de acceso por radio. El usuario móvil puede operar el terminal móvil 100 por medio de un componente 116 de entrada, tal como, por ejemplo, un teclado, y un componente 117 de visor. El funcionamiento del terminal móvil 100 está controlado por una unidad 118 procesadora, que está conectada con una unidad de memoria 119 para almacenar aplicaciones que pueden ser ejecutadas en la unidad 118 procesadora, y para almacenar datos de usuario y de configuración, a los que se accede durante el funcionamiento del terminal móvil 100. El número 130 de referencia se refiere a un sensor con cámara, que es un componente optativo del terminal móvil 100.

A través de una unidad 120 lectora de tarjetas, el terminal móvil 100 está conectado con una tarjeta inteligente 106. La unidad 120 lectora de tarjetas está usualmente dispuesta dentro de un compartimiento de baterías del terminal móvil 200, que es accesible por parte del usuario móvil.

La tarjeta inteligente 106 contiene un módulo de identificador de usuario que proporciona información y funciones para usar el terminal móvil 100 en el sistema de comunicación móvil. En esta realización, la tarjeta inteligente 106, en particular, proporciona información para identificar y autenticar al usuario móvil en la PLMN 102. En particular, el módulo de identificación de usuario puede ser configurado como un SIM, según el estándar de GSM, o como un USIM, según el estándar de UMTS.

La tarjeta inteligente 106 comprende una unidad 121 microprocesadora y una memoria 122 para almacenar códigos de programa ejecutados en el microprocesador 121 y datos usados en el funcionamiento de la tarjeta inteligente 106. Los datos almacenados en la tarjeta inteligente 106 pueden ser leídos y manipulados usando comandos proporcionados por la tarjeta inteligente 106. Una manipulación de los datos puede comprender modificar, borrar o añadir datos. Se proporcionan comandos adicionales para acceder a y ejecutar el código de programa de las aplicaciones almacenadas en la tarjeta inteligente 106. Además, las aplicaciones pueden ser gestionadas mientras la tarjeta inteligente 106 está en uso

del usuario móvil. Esto significa que la tarjeta inteligente 106 proporciona comandos para cargar, instalar, eliminar, bloquear y desbloquear aplicaciones. A los comandos proporcionados por la tarjeta inteligente 106 se puede acceder externamente, en particular, desde el terminal móvil 100. Análogamente, la tarjeta inteligente 106 es capaz de acceder a funciones del terminal móvil 100 usando comandos proactivos. Los comandos proactivos y los comandos para acceder a la tarjeta inteligente 106 pueden ser proporcionados por el llamado Juego de Herramientas de Aplicaciones de SIM (SAT), o por el Juego de Herramientas de Aplicaciones de USIM (USAT), ambos especificados en el documento TS 31.111 del 3GPP. A continuación en la presente memoria, el SAT y el USAT se denominan comúnmente (U)SAT.

En la tarjeta inteligente 106 está habilitado un mecanismo OTA, lo que significa que puede ser establecida una conexión entre la tarjeta inteligente 106 y un sistema de trasfondo. Esto permite una gestión de datos y / o aplicaciones almacenadas en la tarjeta inteligente 106 desde una sede externa. En el caso de gestión de ficheros, el mecanismo se denomina gestión remota de ficheros (RFM) y en el caso de gestión de aplicaciones, el mecanismo se denomina gestión remota de aplicaciones (RAM). Para la RFM y la RAM, puede accederse a un conjunto predefinido de comandos de la tarjeta inteligente 106 desde la sede externa. Este puede ser el conjunto de comandos especificados en el documento TS 23.048 del 3GPP. La RAM y la RAM permiten la actualización de datos almacenados en la tarjeta inteligente 106 y la actualización de aplicaciones existentes, o la descarga de nuevas aplicaciones, en la tarjeta inteligente 106, sin tener que re-emitir la tarjeta inteligente 106.

La gestión remota de la tarjeta inteligente 106 solamente se permite al emisor de la tarjeta, o bien tiene que ser autorizada por el emisor de la tarjeta, que es el operador de la PLMN 102 a la que se ha abonado el usuario móvil. Esto impide a terceros no autorizados acceder a datos sensibles almacenados en la tarjeta inteligente 106, y hacer un uso fraudulento de los mismos.

Según se describe a continuación en la presente memoria, se aplican procedimientos criptográficos para asegurar la RFM y la RAM. Con este fin, se proporciona un servidor 108 OTA en la PLMN 102 que autoriza los accesos a la tarjeta inteligente 106. El servidor 108 OTA está bajo control del operador de la red móvil. Esto significa que solamente el operador de red móvil está autorizado para administrar el servidor 108 OTA, y que el servidor 108 OTA está asegurado contra el acceso por terceros.

Del lado de la tarjeta inteligente 106, los componentes ilustrados en la figura 2 se proporcionan para la RFM y la RAM. En particular, la tarjeta inteligente 106 comprende un componente receptor 201 correspondiente a una interfaz para recibir datos desde un origen externo, tal como, por ejemplo, el terminal móvil 100. El componente receptor 201 está conectado con un componente 202 de descifrado para descifrar información recibida desde el servidor 108 OTA, y con un componente 203 de validación adaptado para validar datos descargados en la tarjeta inteligente 106, usando información criptográfica recibida desde el servidor 108 OTA. Preferiblemente, los componentes 201, 202, 203 de la tarjeta inteligente 106 son módulos de software. Su código de programa está almacenado en la memoria 122 y es ejecutado en el microprocesador 121 de la tarjeta inteligente 106.

Antes de emitir la tarjeta inteligente 106 al usuario móvil, el operador de red móvil genera una o más claves OTA, que son compartidas entre el servidor 108 OTA y la tarjeta inteligente 106. Preferiblemente, existen claves OTA únicas para cada tarjeta inteligente 106 emitida por el operador de red móvil. Para una tarjeta inteligente 106, las claves OTA comprenden una clave para cifrar información, que es usada por el servidor 108 OTA, y una clave para descifrar la información. La clave de descifrado está almacenada con seguridad en la memoria 122 de la tarjeta inteligente 106 y puede ser objeto de acceso por parte del componente 202 de descifrado, al descifrar la información criptográfica proporcionada por el servidor 108 OTA.

En una realización se aplica el cifrado simétrico, donde se usa la misma clave para cifrar y para descifrar datos. Tanto el servidor 108 OTA como la tarjeta inteligente 106 almacenan la clave, que es usada por el servidor 108 OTA para cifrar información, y por la tarjeta inteligente 106 para descifrar información cifrada por el servidor 108 OTA. En otra realización se aplica el cifrado asimétrico, donde se proporciona un par de claves que comprenden una clave de cifrado y una clave de descifrado adjudicada, que es distinta a la clave de cifrado.

Las aplicaciones, u otros datos a descargar en la tarjeta inteligente 106, son proporcionadas por una base 110 de datos, que puede ser operada por el operador de red móvil, o por un tercero. La tarjeta inteligente 106 puede estar conectada con la base 110 de datos mediante la PLMN 102, o mediante otra conexión de datos.

Antes de que las aplicaciones, u otros datos, puedan ser descargadas en la tarjeta inteligente 106, una suma de control de los datos es calculada y proporcionada al servidor 108 OTA, y almacenada en el mismo. La suma de control es una información obtenida de manera unívoca desde el código de programa, tal como, por ejemplo, una función de troceo calculada usando un algoritmo de troceo conocido por una persona experta en la técnica. Además, también se proporciona un Identificador que identifica los datos. El Identificador está compartido entre el servidor 108 OTA y la base 110 de datos. El Identificador es una cadena alfanumérica, que está unívocamente asignada a la aplicación o a los datos.

A continuación, se describe un mecanismo de RAM para descargar una aplicación en la tarjeta inteligente 106. Sin

embargo, la persona experta en la técnica entenderá a partir de la siguiente descripción que un mecanismo de RFM para descargar datos de configuración, u otros datos, en la tarjeta inteligente 106, puede ser implementado de manera análoga.

Tras una correspondiente solicitud, el servidor 108 OTA genera un testigo de seguridad. El testigo de seguridad comprende la suma de control y el Identificador de aplicación de la aplicación a descargar. Después de haber generado el testigo de seguridad, el servidor 108 OTA cifra el testigo de seguridad usando la clave de cifrado descrita anteriormente. Luego, el servidor 108 OTA envía el testigo de seguridad a la tarjeta inteligente 106.

Para transmitir el testigo de seguridad a la tarjeta inteligente, el servidor 108 OTA envía un mensaje que contiene el testigo de seguridad al terminal móvil 100, mediante un canal de comunicación predefinido, y el terminal móvil 100 remite el mensaje a la tarjeta inteligente 106.

Un ejemplo de un canal de comunicación para transmitir el testigo de seguridad es un canal de SMS proporcionado en el sistema de comunicaciones móviles. Para usar el canal de SMS, el servidor 108 OTA genera un mensaje de SMS que contiene el testigo de seguridad y pasa el mensaje de SMS a un centro de servicio de SMS (SMS-C) 112 de la PLMN 102. El SMS-C 112 envía el mensaje de SMS al terminal móvil 100, que recibe el mensaje en la interfaz 115 de radio. Según el procesamiento habitual de mensajes de SMS, el terminal móvil 100 remite luego el mensaje a la tarjeta inteligente 106. Otro ejemplo es una transmisión mediante un GPRS o canal de HSDPA (Acceso por Paquetes de Enlace Descendente de Alta Velocidad) del sistema de comunicación móvil, usando el protocolo independiente del portador (BIP). En general, puede ser usado cualquier canal de comunicación para descargar datos a una tarjeta inteligente 100, conocido por los expertos.

En la tarjeta inteligente 106, el componente receptor 201 recibe el mensaje que contiene el testigo de seguridad y reconoce el testigo de seguridad en base a una característica predefinida del mensaje. La característica puede ser una palabra clave predefinida en la cabecera del mensaje. Después de haber reconocido el testigo de seguridad, el componente receptor 201 pasa el testigo de seguridad al componente 202 de descifrado.

El componente 202 de descifrado descifra el testigo de seguridad usando la precitada clave de descifrado. Si el descifrado es exitoso, el componente 202 de descifrado reconoce un testigo de seguridad válido emitido por el servidor 108 OTA y lo pasa al componente 203 de validación. El descifrado exitoso puede ser confirmado por un mensaje de respuesta generado por el componente 202 de descifrado, que es enviado al servidor 108 OTA. Si el testigo de seguridad no puede ser descifrado exitosamente usando la clave de descifrado predefinida, el testigo de seguridad no es reconocido como válido. La razón para la invalidez puede ser que el testigo de seguridad fue enviado por un tercero no autorizado que no posee la clave de cifrado válida, o que ocurrió un error durante la generación y / o la transmisión del testigo de seguridad desde el servidor 108 OTA a la tarjeta inteligente 106. Por lo tanto, la tarjeta inteligente 106 puede generar un mensaje de error a enviar al servidor 108 OTA, cuando haya sido recibido un testigo de seguridad que no haya sido reconocido como válido. Esto permite al servidor 108 OTA regenerar y reenviar el testigo de seguridad a la tarjeta inteligente 106.

Preferiblemente, el mensaje de respuesta y el mensaje de error son enviados desde el terminal móvil 100 al servidor 108 OTA a través del sistema de comunicación móvil, usando un canal de comunicación predefinido, tal como, por ejemplo, el canal de SMS. Para controlar el terminal móvil 100 a fin de enviar el mensaje de respuesta o el mensaje de error al servidor 108 OTA, la tarjeta inteligente 106 puede usar comandos proactivos del (U)SAT.

El código de programa de la aplicación a descargar en la tarjeta inteligente 106 es transmitido desde la base 110 de datos a la tarjeta inteligente 106, donde es recibido en el componente receptor 201. El componente receptor 201 reconoce el código de programa y lo pasa al componente 203 de validación. Además del código de programa, los datos recibidos comprenden el Identificador de la aplicación, que también es pasado al componente 203 de validación. El procesamiento del código de programa en el componente 203 de validación comprende comparar el Identificador de aplicación con el Identificador de aplicación en el testigo de seguridad, a fin de validar que ha sido recibida la aplicación correcta. Además, el componente 203 de validación valida la integridad de la aplicación recalculando la suma de control y comparando el resultado del cálculo con la suma de control contenida en el testigo de seguridad. Si ambas sumas de control coinciden, el componente 203 de validación autoriza al código de programa para su instalación en la tarjeta inteligente 106. En caso contrario, el componente 203 de validación inhibe la instalación del código de programa. En este caso, el componente 203 de validación puede generar un correspondiente mensaje de error, que es enviado a la base de datos o al servidor 108 OTA.

Para aumentar el nivel de seguridad, una versión cifrada del código de programa puede ser transmitida desde la base 110 de datos a la tarjeta inteligente 106. Esto impide a terceros ver el código de programa durante la transmisión desde la base 110 de datos a la tarjeta inteligente 106. En esta realización, la clave de descifrado para descifrar el código de programa está compartida entre la base 110 de datos y el servidor 108 OTA, y se proporciona a la tarjeta inteligente dentro del testigo de seguridad. El descifrado del código de programa puede ser hecho en el componente 203 de validación de la tarjeta inteligente 106 al comprobar la integridad del código de programa, o en el componente 202 de

descifrado. La suma de control puede ser calculada, bien en base al código de programa llano, o bien en base al código de programa cifrado. En este último caso, el componente 203 de validación calcula la suma de control antes de descifrar el código de programa, mientras que en el primer caso calcula la suma de control después de descifrar el código de programa.

El proceso de descargar la aplicación también está ilustrado esquemáticamente en la figura 3. En las realizaciones ilustradas, la descarga de la aplicación es iniciada por el usuario móvil. El usuario móvil controla el terminal móvil 100 para enviar un mensaje de solicitud a la base 110 de datos en la etapa 301. Al recibir el mensaje de solicitud, la base 110 de datos informa al servidor 108 OTA acerca de la solicitud del usuario móvil en la etapa 302. Esto puede hacerse enviando un mensaje desde la base 110 de datos, enviado al servidor 108 OTA, especificando el Identificador de aplicación. Además, puede darse un código de identificación del usuario móvil en el mensaje, identificando por ello la tarjeta inteligente 106 en la cual ha de descargarse la aplicación. Después de haber recibido el mensaje desde la base 110 de datos, el servidor 108 OTA genera el testigo de seguridad en la etapa 303, si no ha sido generado de antemano. Luego, el testigo de seguridad es enviado desde el servidor 108 OTA a la tarjeta inteligente 106, de la manera descrita anteriormente.

En una realización, después de haber transmitido el testigo de seguridad a la tarjeta inteligente 106, el servidor 108 OTA envía un comando a la base 110 de datos en la etapa 305a, que inicia la transmisión del código de programa desde la base 112 de datos a la tarjeta inteligente 106 en la etapa 306. Alternativamente, el comando para iniciar la transmisión puede ser enviado desde la tarjeta inteligente 106 a la base 110 de datos después de que el testigo de seguridad haya sido recibido en la tarjeta inteligente 106. En la figura 3, esto está ilustrado como la etapa 305b. El comando comprende el Identificador de aplicación y el Identificador de usuario, identificando por ello la aplicación deseada y la tarjeta inteligente 106 en la cual está descargada la aplicación.

Después de haber recibido el código de programa de la aplicación desde la base 110 de datos, la integridad del código de programa es verificada en la tarjeta inteligente 106, en la etapa 307, según lo descrito anteriormente. De antemano, el testigo de seguridad usado para la verificación de integridad está siendo descifrado y validado en la tarjeta inteligente 106 de la manera precitada.

Las realizaciones adicionales difieren de las realizaciones descritas anteriormente en que no es el usuario móvil, sino el servidor 108 OTA, quien inicia la descarga enviando una correspondiente solicitud a la base 110 de datos. Esto permite al operador de red móvil iniciar la descarga y especificar las tarjetas inteligentes 106 en las cuales ha de descargarse la aplicación. El operador de red móvil puede usar esta opción cuando quiere actualizar ciertas tarjetas inteligentes 106 con una nueva aplicación, o una nueva versión de una aplicación ya existente.

Además, es posible que en la etapa 301 de la figura 3 la solicitud para descargar la aplicación no esté dirigida a la base 110 de datos, sino al servidor 108 OTA. En este caso, se omite la etapa 302, en la cual la base de datos informa al servidor 108 OTA acerca de la solicitud de descarga.

Y, por supuesto, también es posible invertir el orden precitado de la transmisión del testigo de seguridad y del código de programa. Así, en realizaciones adicionales, el código de programa de la aplicación es transmitido desde la base 110 de datos a la tarjeta inteligente 106 al principio. En la tarjeta inteligente 106, el código de programa de la aplicación es almacenado temporalmente en la memoria 122 hasta que sea validado. La transmisión del testigo de seguridad desde el servidor 108 OTA a la tarjeta inteligente 106 puede ser iniciada por la base 110 de datos, cuando la base 110 de datos transmite el código de programa de la aplicación a la tarjeta inteligente 106. Con este fin, la base 110 de datos envía un mensaje al servidor OTA que especifica la aplicación y la tarjeta inteligente 106, dando el Identificador de aplicación y el Identificador de usuario del usuario móvil. Como alternativa, la tarjeta inteligente 106 puede extraer el testigo de seguridad del servidor 108 OTA después de haber recibido el código de programa de la aplicación. Para extraer el testigo de seguridad, la tarjeta inteligente 106 envía un mensaje al servidor 108 OTA, mediante el sistema de comunicación móvil, que contiene nuevamente el Identificador de aplicación y el Identificador de usuario.

El canal de comunicación usado para transmitir el código de programa a la tarjeta inteligente 106 depende del tipo de conexión entre la tarjeta inteligente 106 y la base 110 de datos. En principio, puede ser usado cualquier tipo de conexión entre una tarjeta inteligente 106 y la base 110 de datos, conocido para un experto, y los correspondientes canales de comunicación. A continuación en la presente memoria, se describen varios tipos ventajosos de conexión, a modo de ejemplo.

En una realización, la base 110 de datos está conectada con la PLMN 102. La base 110 de datos puede estar conectada directamente con la PLMN 102, o bien puede estar conectada con la PLMN 102 mediante otra red. El código de programa es transmitido desde la base 110 de datos al terminal móvil 110 mediante la PLMN 102, y el terminal móvil 100 remite el código de programa a la tarjeta inteligente 106. La comunicación entre la PLMN 102 y el terminal móvil 100 puede usar cualquier canal de comunicación proporcionado en el sistema de comunicación móvil para el intercambio de datos.

En particular, el código de programa puede ser transmitido al terminal móvil 100 mediante el canal de SMS. Si el volumen

de datos del código de programa supera un único mensaje de SMS, el código de programa es distribuido entre una pluralidad de mensajes concatenados de SMS. Los mensajes concatenados de SMS son remitidos a la tarjeta inteligente 106 en el orden en el que son recibidos en el terminal móvil 100. La tarjeta inteligente 106 almacena temporalmente los mensajes y determina su orden original en base a características contenidas en los mensajes. Luego, la tarjeta inteligente 106 une los mensajes y procesa el mensaje resultante en el componente de validación, según lo descrito anteriormente.

En una arquitectura de sistema en la cual la base de datos y el terminal móvil 100 están conectados a través de la PLMN 102, el código de programa también puede ser transmitido mediante el GPRS, o el canal de HSDPA, del sistema de comunicación móvil, usando el protocolo independiente del portador (BIP). Este canal de comunicación es una alternativa para el canal de SMS, y admite mayores velocidades de transmisión de datos.

En una arquitectura alternativa, la tarjeta inteligente 106 también está conectada con la base 110 de datos a través del terminal móvil 100 que recibe el código de programa en el primer caso, y lo remite a la tarjeta inteligente 106. Sin embargo, la base 110 de datos y el terminal móvil 100 están conectados mediante una red de datos con la cual el terminal móvil 100 está conectado mediante un cierto punto de acceso. La red de datos puede ser Internet, por ejemplo. En una realización de esta arquitectura, el punto de acceso puede ser un punto de acceso de WLAN y el terminal móvil está conectado con el punto de acceso mediante una conexión de WLAN (Red Inalámbrica de Área Local). Otras tecnologías de conexión inalámbrica, tales como, por ejemplo, Bluetooth, ZigBee o NFC (Comunicación de Campo Cercano), pueden ser usadas asimismo para conectar el terminal móvil 100 con el punto de acceso. En otra realización, el punto de acceso es un PC (Ordenador Personal) con acceso a la red de datos. El terminal móvil 100 está conectado con el PC a través de una conexión de USB, por ejemplo.

Por supuesto, el terminal móvil 100 también podría estar conectado con la base de datos directamente de la misma manera, dado que puede estar conectado con el punto de acceso en la arquitectura descrita anteriormente. En esta realización, en la base 110 de datos puede estar incluido en un PC, por ejemplo.

Otro tipo de canal de comunicación para transmitir el código de programa al terminal móvil 100 es un canal de comunicación óptica. Este procedimiento para transferir los datos al terminal móvil 100 hace uso del hecho de que los terminales móviles 100 de hoy están a menudo equipados con sensores 130 con cámara para tomar fotografías, o para videotelefonía. A fin de usar este canal de comunicación, el código de programa puede ser transformado en un código de barras bidimensional o tridimensional que se ilustra en una pantalla. La pantalla está contenida en un dispositivo al cual el código de programa puede ser transmitido desde la base 110 de datos de una manera adecuada. Este dispositivo puede ser un dispositivo de televisión, un PC u otro terminal móvil del mismo tipo que el terminal móvil 100 que contiene la tarjeta inteligente 106, por ejemplo. El código de barras en la pantalla es detectado por medio del sensor 130 con cámara incluido en el terminal móvil 100, y pasado a una aplicación para interpretar el código de barras aplicado, que puede ser ejecutada en el procesador del terminal móvil 100. Después de haber extraído el código de programa del código de barras, es remitido al dispositivo receptor de la tarjeta inteligente 106, que lo pasa al componente de validación a fin de procesar el código de programa de la manera descrita anteriormente.

En realizaciones adicionales, la tarjeta inteligente 106 está conectada directamente con la base 110 de datos. Esto significa que la conexión entre la tarjeta inteligente 106 y la base 110 de datos no está establecida mediante el terminal móvil 100 o una red de datos.

En una realización, esto se logra transfiriendo el código de programa a la tarjeta inteligente 106 usando una lectora externa de tarjetas, que está incluida en un dispositivo con acceso a la base 110 de datos mediante una conexión de datos. La conexión de datos puede ser una conexión directa o una conexión mediante una red de datos.

Sin embargo, para conectar la tarjeta inteligente 106 con la lectora externa de tarjetas, la tarjeta inteligente 106 ha de ser extraída del terminal móvil 100. Esto puede ser inconveniente para el usuario móvil. Este problema puede ser resuelto incluyendo la base 110 de datos en un módulo adaptador 401, que está conectado con la tarjeta inteligente 106, mientras la tarjeta inteligente 106 es insertada en la unidad 120 lectora de tarjetas del terminal móvil 100.

Preferiblemente, el módulo adaptador 401 está conectado entre la unidad 120 lectora de tarjetas del terminal móvil 100 y la tarjeta inteligente 106, según lo ilustrado en la figura 4.

Por tanto, las señales de comunicación entre el terminal móvil 100 y la tarjeta inteligente 106 son intercambiadas mediante el módulo adaptador 401. Aquí, el módulo adaptador 401 puede ser configurado como un dispositivo pasivo, que no está involucrado en la comunicación entre el terminal móvil 100 y la tarjeta inteligente 106. Análogamente, el módulo adaptador 401 puede tener funcionalidades para modificar los mensajes que son intercambiados entre el terminal móvil 100 y la tarjeta inteligente 106.

Para conectar el módulo adaptador 401 entre el terminal móvil 100 y la tarjeta inteligente 106, el módulo adaptador 401 comprende un elemento 402 de contacto, que puede ser insertado en la unidad 120 lectora de tarjetas del terminal móvil 100, y que incluye contactos eléctricos para entrar en contacto con elementos de contacto de la unidad 120 lectora de

tarjetas. Se proporcionan contactos eléctricos 403 adicionales para entrar en contacto con los contactos eléctricos 404 de la tarjeta inteligente 106. Además, el módulo adaptador 401 comprende un microprocesador 405 y una unidad 406 de memoria. El microprocesador 405 es capaz de comunicarse con la tarjeta inteligente 106 y el terminal móvil 100 usando un protocolo de comunicación predefinido. Este puede ser el mismo protocolo de comunicación usado para la comunicación entre el terminal móvil 100 y la tarjeta inteligente 106. Como uno de los contactos eléctricos de la unidad 120 lectora de tarjetas del terminal móvil 100 actúa como una fuente de alimentación para la tarjeta inteligente 106, el microprocesador 405 puede ser alimentado con energía mediante este contacto eléctrico.

En una realización ejemplar, el módulo adaptador 401 comprende un elemento delgado de contacto, que tiene esencialmente la misma forma que la tarjeta inteligente 106, y que puede ser insertado en la unidad 120 lectora de tarjetas del terminal móvil 100, entre los contactos eléctricos de la unidad 120 lectora de tarjetas y la tarjeta inteligente 106. Sobre una superficie, el elemento de contacto comprende elementos 402 de contacto para entrar en contacto con los elementos 404 de contacto de la tarjeta inteligente 106 y, sobre la superficie opuesta, los elementos 402 de contacto están dispuestos para entrar en contacto con los elementos de contacto de la unidad 120 lectora de tarjetas. Los elementos 402, 403 de contacto están conectados con el microprocesador del módulo adaptador 401. El microprocesador 405 y la unidad 406 de memoria del módulo adaptador 401 pueden estar montados sobre una placa de circuitos, que está conectada con el elemento de contacto por medio de un cable flexible, permitiendo por ello colocar la placa de circuitos en el compartimiento de baterías del terminal móvil 100, junto con la batería. Como alternativa, el microprocesador 405 y la unidad 406 de memoria pueden estar incluidos en un chip que está montado sobre el elemento de contacto. En esta realización, la tarjeta inteligente 106 está dotada de un corte para aceptar el chip.

En otra realización, el módulo adaptador 401 comprende un elemento 402 de contacto que tiene esencialmente la misma forma y espesor que la tarjeta inteligente 106, y que puede ser insertado en la unidad 120 lectora de tarjetas del terminal móvil 100 para entrar en contacto con los elementos de contacto de la unidad 120 lectora de tarjetas. El elemento 402 de contacto está conectado con una placa de circuitos mediante uno o más cables flexibles. El microprocesador 405 y la unidad 406 de memoria están montados sobre la placa de circuitos y, además, la placa de circuitos comprende una unidad adicional lectora de tarjetas, conectada con el microprocesador 405 para recibir la tarjeta inteligente 106. La placa de circuitos puede ser lo bastante delgada como para colocarla en el compartimiento de baterías del terminal móvil 100, cuando la tarjeta inteligente 106 es insertada en la unidad 120 lectora de tarjetas.

Usando el módulo adaptador 401, las actualizaciones pueden ser proporcionadas por medio de un dispositivo adicional que el usuario móvil inserta en su terminal móvil 100. En particular, esto mejora la fe de tales usuarios móviles, que sospechan de una transferencia de datos en línea desde una ubicación remota. No obstante, la tarjeta inteligente 106 queda bajo control del operador de red móvil, ya que el testigo de seguridad ha de ser proporcionado por el servidor 108 OTA a fin de validar la aplicación proporcionada por el módulo adaptador 401 antes de la instalación.

Para controlar la descarga de una aplicación en la tarjeta inteligente 106, el módulo adaptador 401, preferiblemente, proporciona una interfaz gráfica de usuario, tal como, por ejemplo, un menú de selección, en la unidad 117 de visor del terminal móvil 100, que permite al usuario seleccionar la aplicación a descargar en la tarjeta inteligente 106. El módulo adaptador 401 controla al terminal móvil 100 para proporcionar la interfaz gráfica de usuario, usando comandos del (U)SAT, por ejemplo. Después de que el usuario ha seleccionado la aplicación deseada, usando la interfaz gráfica de usuario, se inicia el proceso de descarga de la aplicación en la tarjeta inteligente 106.

En este proceso, el módulo adaptador 401 envía el código de programa de la aplicación a la tarjeta inteligente 106. Además, puede generar un mensaje de solicitud para solicitar el testigo de seguridad, y controla al terminal móvil 100 para enviar el mensaje de solicitud al servidor 108 OTA. Luego, el testigo de seguridad adjudicado a la aplicación seleccionada es transmitido desde el servidor 108 OTA a la tarjeta inteligente 106, de la manera descrita anteriormente. Cuando el código de programa de la aplicación y el testigo de seguridad están presentes en la tarjeta inteligente 106, el componente de validación valida el código de programa y permite su instalación, si la validación es exitosa.

Si bien la invención ha sido ilustrada y descrita en detalle en los dibujos y la descripción precedente, tal ilustración y descripción han de ser consideradas ilustrativas o ejemplares, y no restrictivas; la invención no está limitada a las realizaciones reveladas. En particular, la invención no está limitada a una descarga de una aplicación o código de programa en la tarjeta inteligente 106. Una persona experta en la técnica reconocerá que otros datos pueden ser descargados en la tarjeta inteligente 106 de la misma manera en que se ha descrito anteriormente con relación a la descarga de un código de programa de una aplicación. Otras variaciones de las realizaciones reveladas pueden ser entendidas y efectuadas por los expertos en la técnica al poner en práctica la invención reivindicada, a partir de un estudio de los dibujos, la revelación y las reivindicaciones adjuntas.

En las reivindicaciones, la palabra “comprendiendo” no excluye otros elementos o etapas, y el artículo indefinido “un” o “uno” no excluye una pluralidad. Un procesador único, u otra unidad, puede cumplir las funciones de varios elementos enumerados en las reivindicaciones. Un programa de ordenador puede ser almacenado / distribuido en un medio adecuado, tal como un medio de almacenamiento óptico o un medio de estado sólido, suministrado junto con, o como

parte de, otro hardware, pero también puede ser distribuido de otras formas, tal como mediante Internet u otros sistemas de telecomunicación, cableados o inalámbricos. Los signos cualesquiera de referencia en las reivindicaciones no deberían ser interpretados como limitadores de su alcance.

REIVINDICACIONES

1. Un procedimiento para transferir datos a una tarjeta inteligente (106) conectada con un terminal móvil (100) con acceso a una red (102) de comunicación móvil, comprendiendo el procedimiento las etapas de:

- recibir, mediante un primer canal de comunicación, un testigo de seguridad en la tarjeta inteligente (106), desde un servidor (108) conectado con la red (102) de comunicación móvil, comprendiendo el testigo de seguridad una característica de seguridad para validar los datos, y estando cifrado, al menos parcialmente,

- descifrar las partes cifradas del testigo de seguridad en la tarjeta inteligente (106);

- recibir, mediante un segundo canal de comunicación, los datos desde una base (110) de datos en la tarjeta inteligente (106);

- validar los datos en la tarjeta inteligente (106), usando la característica de seguridad contenida en el testigo de seguridad; **caracterizado porque**

los datos están cifrados y la tarjeta inteligente (106) descifra los datos usando una clave de descifrado contenida en el testigo de seguridad.

2. El procedimiento según la reivindicación 1, en el cual la parte cifrada del testigo de seguridad está cifrado usando una clave de cifrado almacenada con seguridad en el servidor (108), y en el cual la parte cifrada del testigo de seguridad es descifrada usando una clave de descifrado adjudicada a la clave de cifrado, estando la clave de descifrado almacenada con seguridad en la tarjeta inteligente (106).

3. El procedimiento según una de las reivindicaciones precedentes, en el cual la característica de seguridad comprende una suma de control de los datos, siendo usada la suma de control en la tarjeta inteligente (106) para validar la integridad de los datos.

4. El procedimiento según una de las reivindicaciones precedentes, en el cual la tarjeta inteligente (106) extrae los datos de la base (110) de datos en respuesta a la recepción del testigo de seguridad, usando información contenida en el testigo de seguridad.

5. El procedimiento según una de las reivindicaciones precedentes, en el cual el servidor (108) envía un comando a la base (110) de datos con relación a la transmisión del testigo de seguridad a la tarjeta inteligente (106), instruyendo el comando a la base (110) de datos para transmitir los datos a la tarjeta inteligente (106).

6. El procedimiento según una de las reivindicaciones precedentes, en el cual el primer canal de comunicación y / o el segundo canal de comunicación es un canal de SMS.

7. El procedimiento según una de las reivindicaciones precedentes, en el cual los datos se proporcionan en una pantalla conectada con la base (110) de datos, y son adquiridos por medio de un sensor (130) con cámara, proporcionado por el terminal móvil (100), y en el cual el terminal móvil (100) pasa los datos adquiridos a la tarjeta inteligente (106).

8. El procedimiento según una de las reivindicaciones precedentes, en el cual los datos son proporcionados en la pantalla en forma codificada, en particular, como un código de barras.

9. Un programa de ordenador cargable en la memoria interna de un ordenador digital, que comprende partes de código de software para realizar las etapas de una de las reivindicaciones 1 a 8 cuando el programa de ordenador es ejecutado en un ordenador.

10. Una tarjeta inteligente (106) para su uso en un terminal móvil (100) con acceso a una red (102) de comunicación móvil, comprendiendo la tarjeta inteligente (106)

- un componente receptor (201) adaptado para recibir, mediante un primer canal de comunicación, un testigo de seguridad desde un servidor (108) conectado con la red (102) de comunicación móvil, y para recibir datos desde una base (110) de datos, mediante un segundo canal de comunicación, comprendiendo el testigo de seguridad un testigo de seguridad para validar los datos, y estando cifrado, al menos parcialmente;

- un componente (202) de descifrado, adaptado para descifrar el testigo de seguridad;

- un componente (203) de validación, adaptado para validar los datos usando la característica de seguridad contenida en el testigo de seguridad; **caracterizada porque** los datos están cifrados y la tarjeta inteligente (106) está configurada para descifrar los datos usando una clave de descifrado contenida en el testigo de seguridad.

11. Un sistema que comprende una tarjeta inteligente (106) según la reivindicación 10, un servidor (108) conectado con la

red (102) de comunicación móvil para transmitir el testigo de seguridad a la tarjeta inteligente (106) y una base (110) de datos conectable con la tarjeta inteligente (106) para transmitir los datos a la tarjeta inteligente (106).

12. El sistema según la reivindicación 11, en el cual la tarjeta inteligente (106) está conectada con la base (110) de datos mediante el terminal móvil (100), estando el terminal móvil (100) conectado con la base (110) de datos mediante la red (102) de comunicación móvil, o una red de datos.

13. El sistema según la reivindicación 11 o 12, en el cual la base (110) de datos está contenida en un módulo adaptador (401), que es conectable con la tarjeta inteligente (106).

14. El sistema según la reivindicación 13, en el cual el módulo adaptador (401) está conectado entre el terminal móvil (100) y la tarjeta inteligente (106).

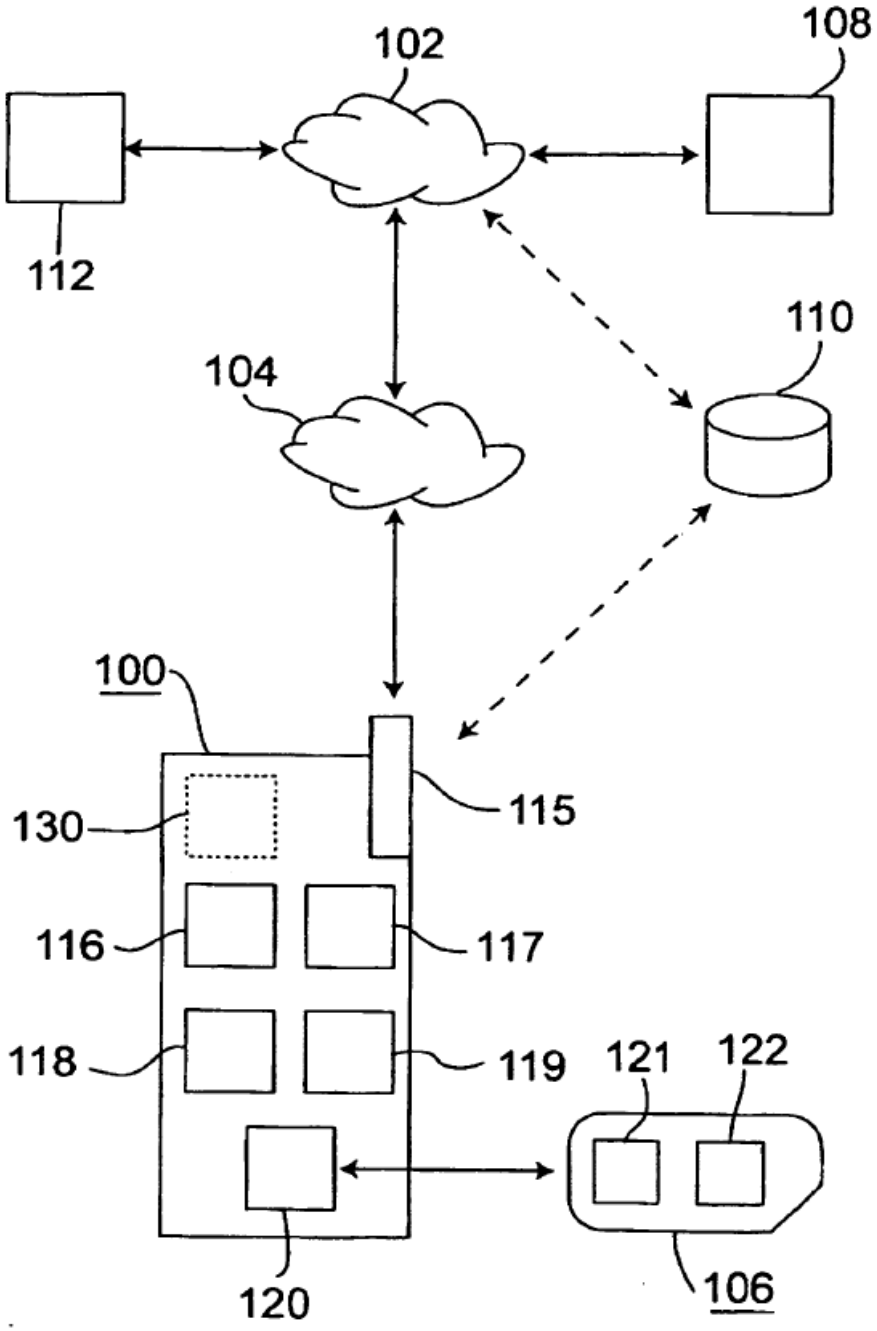

Fig. 1

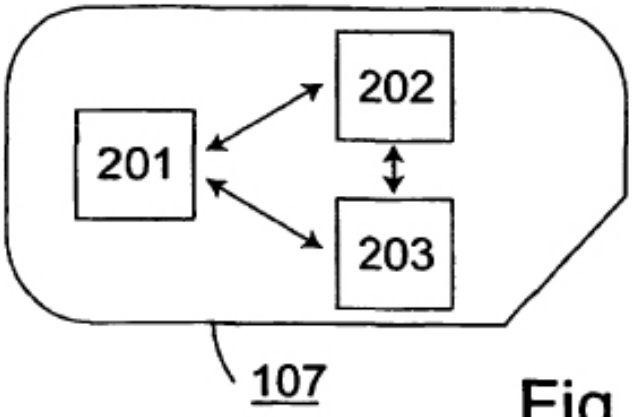
202
201
203
107

Fig. 2

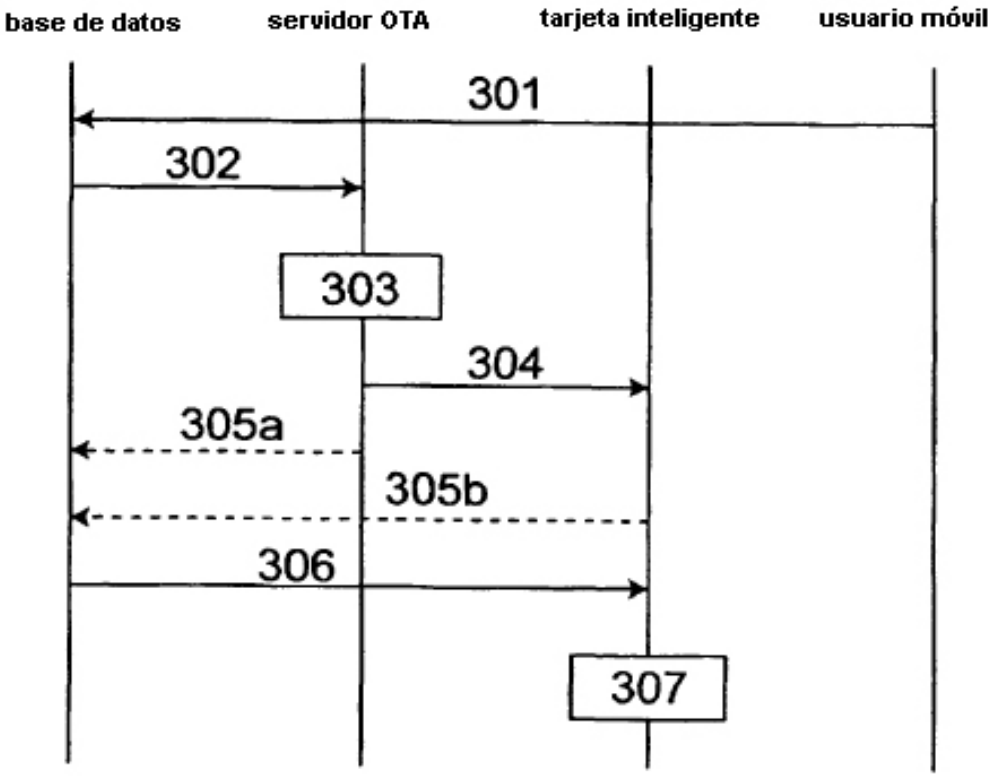
base de datos
servidor OTA
tarjeta inteligente
usuario móvil
301
302
303
304
305a
305b
306
307

Fig. 3

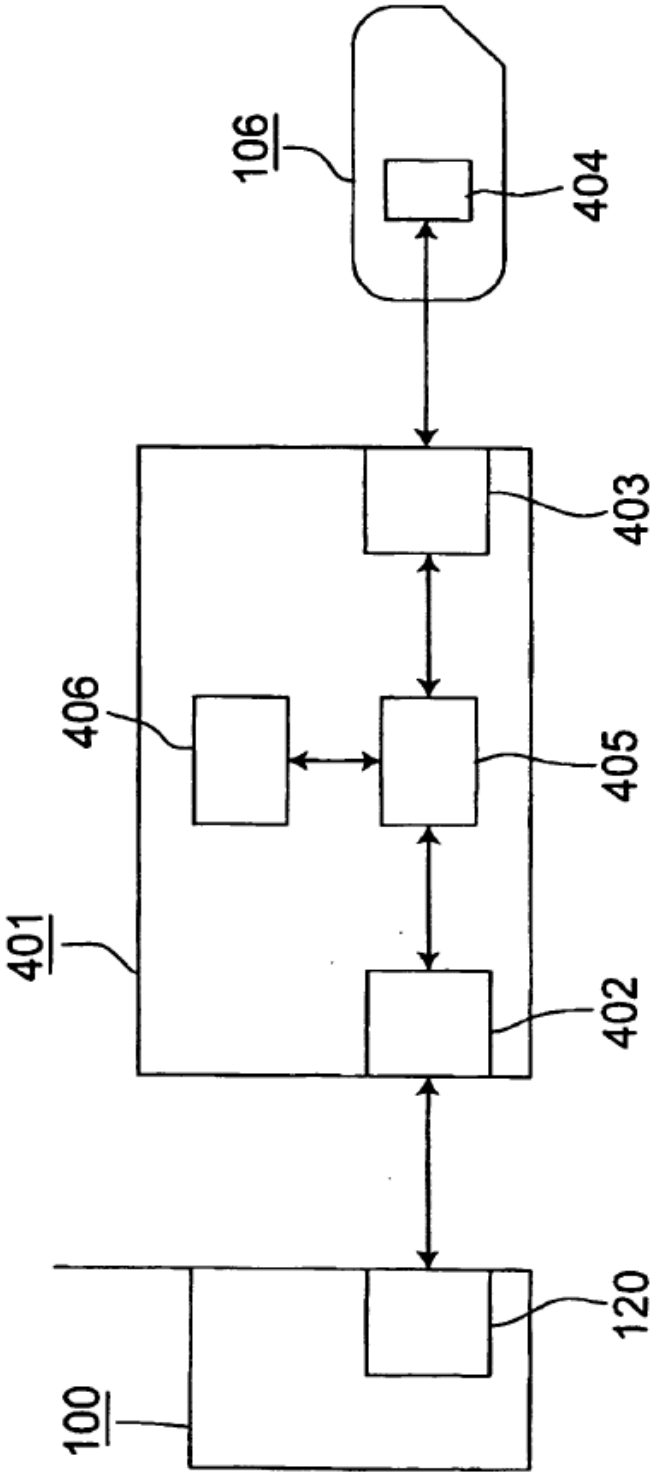

Fig. 4