(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 625 254**

(51) Int. CI.:

H04B 1/3816 (2015.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04W 4/00 (2009.01)
H04W 12/06 (2009.01)
H04W 8/26 (2009.01)
H04W 84/04 (2009.01)
H04W 88/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.11.2012 E 12191036 (8)**

(97) Fecha y número de publicación de la concesión europea: **05.04.2017 EP 2728908**

(54) Título: **Tarjeta con chip de telecomunicaciones**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.07.2017

(73) Titular/es:

MORPHO CARDS GMBH (100.0%)
Konrad-Zuse-Ring 1
24220 Flintbek, DE

(72) Inventor/es:

SHRIYA, SANJEEV y
PHOGAT, VIKAS

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Tarjeta con chip de telecomunicaciones

Campo de la invención

Los dispositivos de telefonía móvil son ubicuos en la sociedad de hoy en día. Muchos individuos llevan al menos un dispositivo de telefonía móvil, típicamente un teléfono celular. También se llevan y usan comúnmente muchos otros dispositivos de telefonía móvil tales como miniordenadores portátiles o tabletas. Mientras el usuario puede comunicar usando un teléfono móvil usando una variedad de diferentes modalidades. Por ejemplo, un usuario puede enviar un SMS, descargar una página web, enviar o recibir un correo electrónico, y/o hacer una llamada de telefonía de voz.

Típicamente los dispositivos de telefonía móvil están adaptados para recibir una tarjeta con chip de telecomunicaciones que proporciona los datos y la autorización necesaria para registrarse en una red de telecomunicaciones móviles celular. La tarjeta con chip de telecomunicaciones se puede mover de un dispositivo de telefonía móvil a otro.

En algunos mercados los individuos pueden usar la misma tarjeta con chip de telecomunicaciones durante años. Otros mercados, tales como en el mundo en desarrollo, las tarjetas con chip de telecomunicaciones se usan durante un periodo de tiempo corto y se desechan. Debido a esto el operador de la red de telecomunicaciones móviles celular puede configurar y permitir constantemente grandes números de tarjetas con chip de telecomunicaciones para sustituir las que se desechan. El operador de red de telecomunicaciones móviles celular también puede cambiar a menudo las opciones de configuración y los datos incluidos en las tarjetas con chip de telecomunicaciones.

Antecedentes y técnica relacionada

El documento EP 2 448 216 A1 se refiere a métodos y a un aparato que permite la programación de información de identificación electrónica de un aparato inalámbrico. En una realización, un aparato inalámbrico comprado o desplegado previamente se activa por una red celular. El aparato inalámbrico se conecta a la red celular usando un módulo de acceso para descargar componentes del sistema operativo y/o componentes del cliente de control de acceso. Los métodos y el aparato descritos permiten actualizaciones, adiciones y sustitución de diversos componentes incluyendo datos de Módulo de Identidad de Abonado Electrónico (eSIM), componentes OS. Una implementación ejemplar de la invención utiliza un intercambio de claves de confianza entre el dispositivo y la red celular para mantener la seguridad.

El documento EP 2 337 307 A2 describe un método, aparato, sistema y producto de programa de ordenador para un servicio de módulo de identidad de abonado seguro. Una comunicación a través de una red móvil se activa en respuesta a recibir una solicitud para activar un servicio de comunicación para el sistema mediante una partición segura del sistema. En respuesta a recibir la solicitud, se recupera una clave para un servicio de permiso desde un almacenamiento accesible solamente por la partición segura. La clave se incluye en un permiso que solicita activar el servicio de comunicación, y el permiso se envía a un proveedor de servicios para el servicio de comunicación. El proveedor de servicios comunica con el servicio de permiso para obtener una firma digital para el permiso. La partición segura recibe un permiso firmado desde el proveedor de servicios, confirma que el permiso firmado contiene la firma digital por el servicio de permiso, y activa el servicio de comunicación para el sistema en respuesta a confirmar que el permiso firmado contiene la firma digital.

Según el documento WO 03/077585 A1 un módulo de identidad se activa de la siguiente manera. Un centro de personalización almacena un código de identidad inicial en el módulo de identidad y comunica el código de identidad inicial a un sistema de gestión de red. Un distribuidor asigna una dirección de comunicación al módulo de identidad y comunica la dirección de comunicación junto con el código de identidad inicial al sistema de gestión de red. El módulo de identidad contacta con el sistema de gestión de red a través de un dispositivo de comunicación (teléfono móvil), por el cual el sistema de gestión de red recibe el código de identidad inicial junto con la dirección de comunicación. El sistema de gestión de red reconoce el código de identidad inicial junto con la dirección de comunicación y, en respuesta, asigna un código de identidad eficaz al módulo de identidad. Posteriormente, el sistema de gestión de red envía un mensaje al dispositivo de comunicación (teléfono móvil). Este mensaje (un SMS especial) comprende el código de identidad eficaz. El módulo de identidad recibe el mensaje a través del dispositivo de comunicación, extrae el código de identidad eficaz del mensaje y almacena el código de identidad eficaz para uso futuro.

Compendio

La invención proporciona una tarjeta con chip de telecomunicaciones, un sistema de actualización, y un método de configuración de una tarjeta con chip de telecomunicaciones en las reivindicaciones independientes. Las realizaciones se dan en las reivindicaciones dependientes.

Como se apreciará por un experto en la técnica, los aspectos de la presente invención se pueden encarnar como un aparato, método o producto de programa de ordenador. Por consiguiente, los aspectos de la presente invención pueden tomar la forma de una realización enteramente hardware, una realización enteramente software (incluyendo microprograma, software residente, microcódigo, etc.) o una realización que combina aspectos software y hardware que todos se pueden conocer de manera general en la presente memoria como un "circuito", "módulo" o "sistema". Además, los aspectos de la presente invención pueden tomar la forma de un producto de programa de ordenador encarnado en uno o más medios legibles por ordenador que tienen código ejecutable por ordenador encarnado en los mismos.

Se puede utilizar cualquier combinación de uno o más medios legibles por ordenador. El medio legible por ordenador puede ser un medio de señal legible por ordenador o un medio de almacenamiento legible por ordenador. Un 'medio de almacenamiento legible por ordenador' como se usa en la presente memoria abarca cualquier medio de almacenamiento tangible que pueda almacenar instrucciones que son ejecutables por un procesador de un dispositivo informático. El medio de almacenamiento legible por ordenador se puede conocer como un medio de almacenamiento no transitorio legible por ordenador. El medio de almacenamiento legible por ordenador también se puede conocer como un medio legible por ordenador tangible. En algunas realizaciones, un medio de almacenamiento legible por ordenador también puede ser capaz de almacenar datos que son capaces de ser accedidos por el procesador del dispositivo informático. Ejemplos de medios de almacenamiento legibles por ordenador incluyen, pero no se limitan a: un disco flexible, una unidad de disco duro magnético, un disco duro de estado sólido, una memoria rápida, una memoria USB, Memoria de Acceso Aleatorio (RAM), Memoria de Sólo Lectura (ROM), un disco óptico, un disco magneto-óptico y el fichero de registro del procesador. Ejemplos de discos ópticos incluyen Discos Compactos (CD) y Discos Versátiles Digitales (DVD), por ejemplo, discos CD-ROM, CD-RW, CD-R, DVD-ROM, DVD-RW o DVD-R. El término medio de almacenamiento legible por ordenador también se refiere a diversos tipos de medios de grabación capaces de ser accedidos por el dispositivo informático a través de una red o un enlace de comunicación. Por ejemplo, un dato se puede recuperar sobre un módem, sobre Internet, o sobre una red de área local. Se puede transmitir código ejecutable por ordenador encarnado en un medio legible por ordenador usando cualquier medio adecuado, incluyendo, pero no limitado a inalámbrico, cableado, cable de fibra óptica, RF, etc., o cualquier combinación adecuada de los precedentes.

Un medio de señal legible por ordenador puede incluir una señal de datos propagada con código ejecutable por ordenador encarnado en el mismo, por ejemplo, en banda base o como parte de una onda portadora. Tal señal propagada puede tomar cualquiera de una variedad de formas, incluyendo, pero no limitada a, electromagnética, óptica, o cualquier combinación adecuada de las mismas. Un medio de señal legible por ordenador puede ser cualquier medio legible por ordenador que no sea un medio de almacenamiento legible por ordenador y que puede comunicar, propagar, o transportar un programa para uso por o en conexión con un sistema, aparato o dispositivo de ejecución de instrucciones.

'Memoria de ordenador', 'memoria', o 'medio de memoria' es un ejemplo de un medio de almacenamiento legible por ordenador. Memoria de ordenador es cualquier memoria que sea directamente accesible por un procesador. 'Almacenamiento de ordenador' o 'almacenamiento' es un ejemplo adicional de un medio de almacenamiento legible por ordenador. Almacenamiento de ordenador es cualquier medio de almacenamiento legible por ordenador no volátil. En algunas realizaciones almacenamiento de ordenador también puede ser memoria de ordenador o viceversa.

Un 'procesador' o 'medio de procesador' como se usa en la presente memoria abarca un componente electrónico que es capaz de ejecutar un programa o instrucción ejecutable por máquina o código ejecutable por ordenador. Las referencias al dispositivo informático que comprenden "un procesador" se deberían interpretar como que contienen posiblemente más de un procesador o núcleo de procesador. El procesador puede ser por ejemplo un procesador de múltiples núcleos. Un procesador también puede referirse a una colección de procesadores dentro de un único sistema informático o distribuido entre múltiples sistemas informáticos. El término dispositivo informático también se debería interpretar para referirse posiblemente a una colección o red de dispositivos informáticos cada uno que comprende un procesador o procesadores. El código o programa ejecutable por ordenador se puede ejecutar por múltiples procesadores que pueden estar dentro del mismo dispositivo informático o que se pueden distribuir incluso a través de múltiples dispositivos informáticos.

Un código ejecutable por ordenador puede comprender instrucciones ejecutables por máquina o un programa que hace a un procesador realizar un aspecto de la presente invención. Un código ejecutable por ordenador para llevar a cabo operaciones para aspectos de la presente invención se puede escribir en cualquier combinación de uno o más lenguajes de programación, incluyendo un lenguaje de programación orientado a objetos tal como Java, Smalltalk, C++ o similares y lenguajes de programación de procedimiento convencional, tales como el lenguaje de programación "C" o lenguajes de programación similares y compilados en instrucciones ejecutables por máquina. En algunos casos el código ejecutable por ordenador puede ser en forma de un lenguaje de alto nivel o en una forma precompilada y puede ser usado en conjunto con un intérprete que genera las instrucciones ejecutables por máquina sobre la marcha.

El código ejecutable por ordenador puede ejecutarse totalmente en el ordenador del usuario, parcialmente en el ordenador del usuario, como un paquete software autónomo, parcialmente en el ordenador del usuario y

parcialmente en un ordenador remoto o totalmente en el ordenador o servidor remoto. En este último escenario, el ordenador remoto se puede conectar al ordenador del usuario a través de cualquier tipo de red, incluyendo una red de área local (LAN) o una red de área amplia (WAN), o la conexión se puede hacer a un ordenador externo (por ejemplo, a través de Internet usando un Proveedor de Servicios de Internet).

Los aspectos de la presente invención se describen con referencia a ilustraciones del diagrama de flujo y/o diagramas de bloques de métodos, aparato (sistemas) y productos de programa de ordenador según realizaciones de la invención. Se entenderá que cada bloque o una parte de los bloques del diagrama de flujo, las ilustraciones, y/o los diagramas de bloques, se pueden implementar mediante instrucciones de programa de ordenador en forma de código ejecutable por ordenador cuando sea aplicable. Se entiende además que, cuando no son mutuamente exclusivas, se pueden combinar combinaciones de bloques en diferentes diagramas de flujo, ilustraciones, y/o diagramas de bloques. Estas instrucciones de programa de ordenador se pueden proporcionar a un procesador de un ordenador de propósito general, ordenador de propósito especial, u otro aparato de procesamiento de datos programable para producir una máquina, de manera que las instrucciones, que se ejecutan a través del procesador del ordenador u otro aparato de procesamiento de datos programable, creen medios para implementar las funciones/acciones especificadas en el bloque o bloques del diagrama de flujo y/o diagrama de bloques.

Estas instrucciones de programa de ordenador también se pueden almacenar en un medio legible por ordenador que puede dirigir un ordenador, otro aparato de procesamiento de datos programable, u otros dispositivos a funcionar de una manera particular, de manera que las instrucciones almacenadas en el medio legible por ordenador producen un artículo de fabricación que incluye instrucciones que implementan la función/acción especificada en el bloque o bloques del diagrama de flujo y/o diagrama de bloques.

Las instrucciones de programa de ordenador también se pueden cargar sobre un ordenador, otro aparato de procesamiento de datos programable, u otros dispositivos para hacer que una serie de pasos de operación sean realizados en el ordenador, otro aparato programable u otros dispositivos produzcan un proceso implementado por ordenador de manera que las instrucciones que se ejecutan en el ordenador u otro aparato programable proporcionen procesos para implementar las funciones/acciones especificadas en el bloque o bloques del diagrama de flujo y/o diagrama de bloques.

Una ‘interfaz de usuario’ como se usa en la presente memoria es una interfaz que permite a un usuario u operador interaccionar con un ordenador o sistema informático. Una ‘interfaz de usuario’ también se puede conocer como un ‘dispositivo de interfaz humana’. Una interfaz de usuario puede proporcionar información o datos al operador y/o recibir información o datos desde el operador. Una interfaz de usuario puede permitir que la entrada de un operador sea recibida por el ordenador y puede proporcionar salida al usuario desde el ordenador. En otras palabras, la interfaz de usuario puede permitir a un operador controlar o manipular un ordenador y la interfaz puede permitir al ordenador indicar los efectos del control o manipulación del operador. El visualizador de datos o información en un visualizador o una interfaz gráfica de usuario es un ejemplo de suministro de información a un operador. La recepción de datos a través de un teclado, ratón, bola de apuntamiento, almohadilla táctil, dispositivo de puntero, tableta de gráficos, palanca de mando, almohadilla de juegos, cámara web, auriculares, palancas de cambios, volante, pedales, guante cableado, alfombrilla de baile, mando a distancia, y acelerómetro todos son ejemplos de componentes de interfaz de usuario que permiten la recepción de información o datos desde un operador.

Una ‘tarjeta con chip de telecomunicaciones’ como se usa en la presente memoria es una tarjeta con chip que permite el registro de un dispositivo de telefonía móvil en una red de telecomunicaciones móviles celular digital. Por ejemplo, una tarjeta con chip de telecomunicaciones puede ser un módulo de identidad de abonado (SIM) que almacena de manera segura una clave de abonado al servicio que se usa para identificar al abonado en la red de telecomunicaciones móviles celular digital.

Un ‘dispositivo de telefonía móvil’ como se usa en la presente memoria es un dispositivo de comunicación móvil adaptado para conectarse a y proporcionar acceso a una red de telecomunicaciones móviles celular digital. Ejemplos de un dispositivo de telefonía móvil incluye, pero no se limitan a: un teléfono móvil, un asistente personal digital, un buscapersonas, un módem celular para un ordenador, un miniordenador portátil, un ordenador portátil, una tableta, y un libro electrónico o lector de documentos.

En un aspecto la invención proporciona una tarjeta con chip de telecomunicaciones para permitir el registro de un dispositivo de telefonía móvil en una red de telecomunicaciones móviles celular digital. La tarjeta con chip de telecomunicaciones comprende una interfaz de lector de tarjeta con chip adaptada para permitir una comunicación entre la tarjeta con chip de telecomunicaciones y el dispositivo de telefonía móvil. La interfaz de lector de tarjeta con chip se puede usar alternativamente o también para permitir una comunicación entre la tarjeta con chip de telecomunicaciones y un dispositivo terminal para programar o actualizar la tarjeta con chip de telecomunicaciones. La tarjeta con chip de telecomunicaciones además comprende un medio de procesador de tarjeta con chip. El procesador de tarjeta con chip también puede ser simplemente un procesador o un procesador de tarjeta con chip en algunas realizaciones. La tarjeta con chip de telecomunicaciones además comprende un medio de memoria segura o una memoria segura para almacenar programas para ejecución por el medio de procesador de tarjeta con chip. El medio de memoria segura es un medio de memoria o memoria que no es accesible directamente a través de la interfaz de lector de tarjeta con chip.

El medio de procesador de tarjeta con chip es capaz de comunicar a través de la interfaz de lector de tarjeta con chip y el propio medio de procesador de tarjeta con chip puede añadir o borrar los contenidos del medio de memoria segura. La tarjeta con chip de telecomunicaciones además comprende un programa almacenado en el medio de memoria segura. El programa comprende instrucciones legibles por máquina ejecutables por el medio de procesador de tarjeta con chip. La ejecución del programa hace al medio de procesador de tarjeta con chip realizar una primera autenticación mutua criptográfica entre la tarjeta con chip de telecomunicaciones y un dispositivo terminal a través de la interfaz de lector de tarjeta con chip. El dispositivo terminal tiene un lector de tarjeta con chip operable para conectar a la interfaz de lector de tarjeta con chip. Una autenticación mutua criptográfica como se usa en la presente memoria abarca un algoritmo donde los métodos criptográficos se usan para dos dispositivos para autenticar la identidad o validez uno de otro. Una autenticación mutua criptográfica puede implicar también un intercambio de clave o una validación de claves criptográficas.

La ejecución del programa además hace al medio de procesador de tarjeta con chip recibir un mensaje de configuración a través de la interfaz de lector de tarjeta con chip. La ejecución del programa además hace al medio de procesador de tarjeta con chip almacenar el mensaje de configuración en el medio de memoria segura. La ejecución del programa además hace al medio de procesador de tarjeta con chip borrar el programa del medio de memoria. Por ejemplo, el programa se podría cargar en una memoria dentro del medio de procesador de tarjeta con chip y después de la ejecución del programa se borra a sí mismo. Alternativamente el programa podría tener un subprograma pequeño o porción de instrucciones ejecutables que se pueden cargar en el medio de procesador de tarjeta con chip y hace al programa ser borrado del medio de memoria. Esta realización puede ser beneficiosa debido a que proporciona un medio de personalización de la tarjeta con chip de telecomunicaciones antes de la instalación en el dispositivo de telefonía móvil. Borrar el programa del medio de memoria puede ser beneficioso debido a que elimina la amenaza de que un pirata informático u otro individuo que usa el programa clone la tarjeta con chip de telecomunicaciones o modifique su contenido. La tarjeta con chip de telecomunicaciones se puede modificar solamente una vez usando esta técnica. Esto proporciona un alto nivel de seguridad al tiempo que permite una personalización completa de la tarjeta con chip de telecomunicaciones.

En otra realización la ejecución de las instrucciones hace además al medio de procesador de tarjeta con chip realizar cualquiera de las siguientes: realizar una autenticación MAC del mensaje de configuración, verificar la firma digital del mensaje de configuración, descifrar el mensaje de configuración, y combinaciones de las mismas. Por ejemplo, el programa puede contener claves criptográficas que permitan el descifrado de un mensaje de configuración cifrado. Esto proporciona una capa de seguridad adicional. Por ejemplo, si el mensaje de configuración está cifrado y se descifra por el programa entonces esto asegura al fabricante de la tarjeta con chip de telecomunicaciones que el mensaje de configuración se puede colocar en la tarjeta con chip en una memoria segura de manera segura. Por ejemplo, las tarjetas con chip de telecomunicaciones se pueden distribuir y proporcionar a un punto de reventa. Por ejemplo, la tarjeta con chip de telecomunicaciones se puede distribuir a un punto de reventa y el punto de reventa se puede dotar con un dispositivo terminal para interconectar con la interfaz de lector de tarjeta con chip. El punto de reventa no necesita tener ninguna de las claves necesarias para cifrar o descifrar el mensaje de configuración. El mensaje de configuración se puede generar por un servidor central y entonces enviar a través del dispositivo terminal a la tarjeta con chip de telecomunicaciones que entonces descifra el mensaje. Siempre que el servidor central no llegue a estar comprometido el descifrado del mensaje de configuración puede asegurar que el mensaje de configuración es auténtico y está inalterado.

En otra realización el mensaje de configuración es cualquiera de los siguientes: un conjunto de números de teléfono, información de abonado, un sistema operativo, datos de anuncio, una aplicación, y combinaciones de los mismos. En otras palabras, los contenidos del medio de memoria segura se pueden personalizar completamente. El mensaje de configuración puede ser datos o información que se puede escribir directamente en el medio de memoria segura por el procesador. La información de abonado como se usa en la presente memoria abarca datos o claves o información que se usa por un dispositivo de telefonía móvil para registrarse en la red de telecomunicaciones móviles.

En otra realización la ejecución de las instrucciones hace al medio de procesador de tarjeta con chip borrar el medio de memoria segura antes de almacenar el mensaje de configuración en el medio de memoria segura. Esta realización proporciona un nivel de seguridad incluso más alto debido a que se han borrado todos los contenidos del medio de memoria segura. Esto reduce la posibilidad de que el código que permanece en el medio de procesador de tarjeta con chip se puede explotar para identificar o tomar el control de la tarjeta con chip de telecomunicaciones. Esto reduce la posibilidad de que se pueda piratear la tarjeta con chip de telecomunicaciones.

En otra realización, la tarjeta con chip de telecomunicaciones comprende una memoria interna dentro del medio de procesador de tarjeta con chip. Dentro de la memoria interna se puede cargar una porción o el programa entero en la tarjeta con chip y usar. Esta memoria interna es una memoria volátil de modo que cualquier cosa almacenada en ella no se almacena permanentemente.

En otra realización, el medio de memoria segura es un medio de memoria no volátil. En otras palabras, los datos y la información almacenados en el medio de memoria segura son persistentes y permanecen incluso si se quita la alimentación de la tarjeta con chip de telecomunicaciones.

En otro aspecto, la invención proporciona un sistema de actualización para modificar la tarjeta con chip de telecomunicaciones. La tarjeta con chip de telecomunicaciones es según una realización de la invención. El sistema de actualización comprende un dispositivo terminal. El dispositivo terminal comprende un lector de tarjeta con chip operable para recibir la tarjeta con chip de telecomunicaciones y para intercambiar datos con la interfaz de lector de tarjeta con chip. Esencialmente, la tarjeta con chip de telecomunicaciones es capaz de ser insertada en el lector de tarjeta con chip de manera que el sistema de actualización pueda intercambiar datos con ella. El dispositivo terminal comprende además un medio de procesador de dispositivo terminal. El medio de procesador de dispositivo terminal puede ser también un procesador de dispositivo terminal o simplemente un procesador como se definió anteriormente.

El dispositivo terminal comprende además un medio de memoria de terminal o memoria de terminal para almacenar un programa de medio de terminal. El medio de memoria de terminal puede ser una memoria de ordenador como se define en la presente memoria. La ejecución del programa de medio de terminal hace al medio de procesador de terminal realizar una primera autenticación mutua criptográfica entre el dispositivo terminal y la tarjeta con chip de telecomunicaciones a través de la interfaz de lector de tarjeta con chip. La ejecución del programa de medio de terminal hace al medio de procesador de terminal realizar una segunda autenticación mutua criptográfica entre el dispositivo terminal y un servidor. Por ejemplo, el dispositivo terminal se puede conectar a un servidor a través de cualquier número de redes de telecomunicaciones o modos de comunicación, dado que el dispositivo terminal se puede conectar a través de una red de telecomunicaciones móviles celular digital o a través de Internet. El servidor puede ser un servidor central que se usa para generar el método de configuración.

La ejecución del programa de medio de terminal hace al medio de procesador de terminal enviar un testigo de seguridad criptográfico al servidor. En algunas realizaciones, el testigo de seguridad criptográfico es un identificador que identifica a un abonado. La ejecución de las instrucciones hace además al procesador solicitar un mensaje de servidor criptográfico desde el servidor. En algunas realizaciones, el servidor puede seleccionar el mensaje de servidor criptográfico usando el testigo de seguridad criptográfico. El mensaje de servidor criptográfico también se puede personalizar en algunas realizaciones dependiendo del testigo de seguridad criptográfico. Por ejemplo, si el testigo de seguridad criptográfico identifica un abonado, los datos de abonado que enlazan el registro del dispositivo de telefonía móvil con una cuenta del abonado se pueden incluir en el mensaje de servidor criptográfico.

La ejecución del programa de medio de terminal hace además al medio de procesador de terminal recibir un mensaje de servidor criptográfico desde el servidor. La ejecución del programa de medio de terminal hace además al medio de procesador de terminal descifrar el mensaje de servidor criptográfico usando una clave criptográfica. En diversas realizaciones esto se puede realizar de diferentes formas. En algunas realizaciones, el descifrado se puede realizar sobre la marcha y el mensaje descifrado se puede escribir directamente en el medio de memoria de seguridad. En otras realizaciones se recibe el mensaje de servidor criptográfico entero y luego se descifra más tarde.

La ejecución del programa de medio de terminal hace además al medio de procesador de terminal construir un mensaje de configuración usando el mensaje de servidor criptográfico descifrado. En algunas realizaciones, el mensaje de configuración es un mensaje no cifrado que se almacena directamente en el medio de memoria segura. En otras realizaciones, se puede cifrar el mensaje de configuración. Por ejemplo, el mensaje de servidor criptográfico se puede cifrar dos veces. El servidor envía el mensaje de servidor criptográfico al dispositivo terminal que entonces lo descifra. Esto asegura que solamente el dispositivo terminal específico puede recibir y usar el mensaje de servidor criptográfico. A continuación, el mensaje de servidor criptográfico descifrado es de hecho un mensaje de configuración cifrado. Este mensaje de configuración cifrado se transfiere entonces desde el dispositivo terminal a la tarjeta con chip de telecomunicaciones donde se descifra finalmente y se coloca en la memoria segura. La ejecución del programa de medio de terminal hace además al medio de procesador de terminal enviar el mensaje de configuración a la tarjeta con chip de telecomunicaciones a través de la interfaz de lector de tarjeta con chip.

En otra realización, el dispositivo terminal comprende un lector de huella dactilar para escanear una huella dactilar de un operador.

En otra realización, el dispositivo terminal comprende un medio de medición biométrica para medir un parámetro biométrico de un abonado.

En otra realización, el dispositivo terminal comprende además un registro de huella dactilar almacenado en el medio de memoria de dispositivo terminal. La ejecución del programa de medio de terminal hace además al procesador de terminal verificar la huella dactilar comparando la huella dactilar con el registro de huella dactilar. La ejecución del programa de medio de terminal hace además al medio de procesador de terminal abortar la solicitud del mensaje de servidor criptográfico a menos que se verifique la huella dactilar. Esta realización se puede usar para asegurar que solamente el operador previsto del dispositivo terminal es capaz de cargar el mensaje de configuración sobre la tarjeta con chip de telecomunicaciones. El registro de huella dactilar podría ser una huella dactilar de una persona que opera el dispositivo terminal en un punto de reventa. En otras realizaciones, el registro de huella dactilar se podría transferir, por ejemplo, a través de cifrado desde el servidor al dispositivo terminal. Un abonado entonces escanearía su huella dactilar en el lector de huella dactilar y ésta se compararía. Esto aseguraría que el abonado esté presente realmente cuando se realiza la actualización de la tarjeta con chip de telecomunicaciones.

En otra realización, el testigo de seguridad comprende la huella dactilar.

En otra realización, el testigo de seguridad comprende el parámetro biométrico medido por el dispositivo de medición biométrica.

En otra realización, el sistema de actualización comprende además un lector de tarjeta inteligente operable para interconectar con una tarjeta inteligente. La ejecución del programa de medio de terminal hace además al medio de memoria de terminal realizar una validación criptográfica de la tarjeta inteligente. La ejecución del programa de medio de terminal hace además al medio de procesador de terminal abortar la solicitud del mensaje de servidor criptográfico a menos que se valide la tarjeta inteligente.

En otra realización, la tarjeta inteligente comprende o contiene una memoria de tarjeta inteligente que contiene un testigo de identidad. El testigo de identidad comprende cualquiera de los siguientes: datos de huella dactilar almacenados, datos biométricos, datos de escaneado de iris, autenticación criptográfica, claves o pares de claves criptográficas, y combinaciones de los mismos. La ejecución del programa de medio de terminal hace además al medio de procesador de terminal recuperar un testigo de identidad de la memoria de tarjeta inteligente a través del lector de tarjeta inteligente. El testigo de seguridad comprende el testigo de identidad.

En otra realización, el dispositivo terminal comprende además una interfaz de usuario. La ejecución de las instrucciones hace además al procesador de terminal recibir datos de usuario desde la interfaz de usuario. El testigo de seguridad comprende los datos de usuario. Por ejemplo, los datos de usuario podrían ser un número de identificación personal o también podrían ser algún tipo de otra identificación o contraseña de usuario. Esto puede ser beneficioso para enlazar el mensaje de configuración con una cuenta de un abonado.

En otra realización, el sistema de actualización comprende el servidor.

En otro aspecto, la invención proporciona un método de configuración de una tarjeta con chip de telecomunicaciones usando un sistema de actualización. La tarjeta con chip de telecomunicaciones comprende una interfaz de lector de tarjeta con chip adaptada para permitir una comunicación entre la tarjeta con chip de telecomunicaciones y el dispositivo de telefonía móvil. La tarjeta con chip de telecomunicaciones comprende además un medio de procesador de tarjeta con chip. La tarjeta con chip de telecomunicaciones comprende además un medio de memoria segura para almacenar programas para su ejecución por el medio de procesador de tarjeta con chip. La tarjeta con chip de telecomunicación comprende además un programa almacenado en el medio seguro que comprende instrucciones legibles por máquina ejecutables por el medio de procesador de tarjeta con chip. El sistema de actualización comprende un dispositivo terminal. El dispositivo terminal comprende un lector de tarjeta con chip operable para recibir la tarjeta con chip de telecomunicaciones y para intercambiar datos con la interfaz de lector de tarjeta con chip. El dispositivo terminal comprende un medio de procesador de dispositivo terminal. El método comprende el paso de realizar una primera autenticación mutua criptográfica entre el dispositivo terminal y la tarjeta con chip de telecomunicaciones usando la interfaz de lector de tarjeta con chip.

El medio de procesador de dispositivo terminal y el medio de procesador de tarjeta con chip realizan esto. El método comprende además el paso de realizar una segunda autenticación mutua criptográfica entre el dispositivo terminal y un servidor. El método comprende además el paso de enviar el testigo de seguridad criptográfico desde el dispositivo terminal al servidor. El método comprende además el paso de enviar una solicitud de mensaje de servidor criptográfico desde el dispositivo terminal al servidor. El método comprende además el paso de enviar el mensaje de servidor criptográfico desde el servidor al dispositivo terminal. El método comprende además el paso de descifrar el mensaje de servidor criptográfico usando la clave criptográfica. El método comprende además el paso de construir un mensaje de configuración usando el mensaje de servidor criptográfico descifrado. El método comprende además el paso de enviar el mensaje de configuración desde el dispositivo terminal a la tarjeta con chip de telecomunicaciones. El método comprende además el paso de almacenar el mensaje de configuración en el medio de memoria segura. El método comprende además el paso de borrar el programa del medio de memoria.

En otra realización, el método comprende además identificar el abonado usando el testigo de seguridad criptográfico. Esto se puede realizar por el servidor. En otra realización, el testigo de seguridad comprende un identificador biométrico tal como una huella dactilar o un escaneado de iris. El abonado se identifica comparando el identificador biométrico con una base de datos biométrica.

Se entiende que una o más de las realizaciones antes mencionadas de la invención se pueden combinar siempre que las realizaciones combinadas no sean mutuamente exclusivas.

Breve descripción de los dibujos

En lo siguiente se explican con mayor detalle realizaciones de la invención, a modo de ejemplo solamente, haciendo referencia a los dibujos en los que:

la Fig. 1 ilustra el uso de una tarjeta con chip de telecomunicaciones;

la Fig. 2 ilustra un método según una realización de la invención;

la Fig. 3 ilustra una tarjeta con chip de telecomunicaciones 100 antes de la modificación por un sistema de actualización;

la Fig. 4 muestra la misma tarjeta con chip de telecomunicaciones que se mostró en la Fig. 3 después de una modificación por un sistema de actualización;

la Fig. 5 muestra un sistema de actualización según una realización de la invención;

la Fig. 6 muestra un ejemplo adicional de un sistema de actualización;

la Fig. 7 muestra un ejemplo adicional de un sistema de actualización;

la Fig. 8 muestra una ilustración funcional de un sistema de actualización;

la Fig. 9 muestra un ejemplo de la posible conectividad entre el proveedor de tarjeta con chip de telecomunicaciones y diversos proveedores de servicios de telecomunicaciones;

la Fig. 10 Ilustra una arquitectura TMS para actualizar el software en el dispositivo terminal.

la Fig. 11 ilustra un método de un protocolo de comunicación entre un dispositivo terminal y un servidor;

la Fig.12 ilustra un mecanismo de una miniaplicación que procesa los comandos de actualización que se reciben por el terminal en forma cifrada y entonces se pasan a la miniaplicación para descifrado y procesamiento adicional por el Sistema Operativo de tarjeta.

la Fig. 13 ilustra un protocolo de comunicación entre un dispositivo terminal y una tarjeta inteligente;

la Fig. 14 muestra un diagrama de bloques que ilustra un método de generación de una Clave Individual de Tarjeta; y

la Fig. 15 ilustra un método de un inicio de diálogo SSL entre un cliente SSL y un servidor SSL.

Descripción detallada

Los elementos numerados iguales en estas figuras son o bien elementos equivalentes o bien realizan la misma función. Los elementos que han sido discutidos previamente no serán necesariamente discutidos en figuras posteriores si la función es equivalente.

La Fig. 1 ilustra el uso de una tarjeta con chip de telecomunicaciones 100. La tarjeta con chip de telecomunicaciones 100 se muestra como que tiene una interfaz de lector de tarjeta con chip 102. La tarjeta con chip de telecomunicaciones 100 se ha insertado en un dispositivo de telefonía móvil 104. El dispositivo de telefonía móvil 104 comprende un lector de tarjeta con chip 106 que se conecta con la interfaz de lector de tarjeta con chip. La tarjeta con chip de telecomunicaciones 100 permite que el dispositivo de telefonía móvil 104 se registre en y se comunique con una red de telecomunicaciones móviles celular digital 107. El dispositivo de telefonía móvil 104 tiene un enlace radio 108 a la red de telecomunicaciones móviles celular digital 107. Por ejemplo, la red de telecomunicaciones móviles celular digital 107 puede comprender una estación base 110. La estación base es operable para conectarse al dispositivo de telefonía móvil 104 a través del enlace radio 108. La estación base 110 se conecta a un controlador de red radio 112. El controlador de red radio 112 está conectado entonces a una red de telecomunicaciones 114. La red de telecomunicaciones móviles celular digital 107 puede proporcionar por lo tanto acceso a otras redes de telecomunicaciones, tales como Internet, la red de voz de telefonía global, u otras redes de comunicaciones 114.

La Fig. 2 ilustra un método según una realización de la invención. En primer lugar, en el paso 200 se realiza una primera autenticación mutua criptográfica entre un dispositivo terminal y una tarjeta con chip de telecomunicaciones usando una interfaz de lector de tarjeta con chip. A continuación, en el paso 202, se realiza una segunda autenticación mutua criptográfica entre el dispositivo terminal y un servidor. Los pasos 202 y 200 se pueden realizar en cualquier orden. A continuación, en el paso 204, se envía un testigo de seguridad criptográfico desde el dispositivo terminal al servidor. A continuación, en el paso 206, se envía una solicitud de mensaje de servidor criptográfico desde el dispositivo terminal al servidor. A continuación, en el paso 208 se envía un mensaje de servidor criptográfico desde el servidor al dispositivo terminal. A continuación, en el paso 210 el mensaje de servidor criptográfico se descifra usando una clave criptográfica. En el paso 212 se construye un mensaje de configuración usando el mensaje de servidor criptográfico descifrado. En algunas realizaciones la construcción del mensaje de configuración puede ser simplemente proporcionando el mensaje de servidor criptográfico descifrado. A continuación, en el paso 214 el mensaje de configuración se envía desde el dispositivo terminal a la tarjeta con chip de telecomunicaciones. A continuación, en el paso 216 el mensaje de configuración se almacena en el medio de memoria segura. En algunas realizaciones hay un paso adicional de descifrado del mensaje de configuración. A continuación, en el paso 218, se borra un programa que estaba operando en la tarjeta con chip de telecomunicaciones. El programa era operable para almacenar el mensaje de configuración en el medio de memoria segura.

La Fig. 3 ilustra una tarjeta con chip de telecomunicaciones 100. La tarjeta con chip de telecomunicaciones 100 mostrada en la Fig. 3 es antes de que se haya modificado por un sistema de actualización. La tarjeta con chip de telecomunicaciones 100 muestra la interfaz de lector de tarjeta con chip 102 conectada a un medio de procesador de tarjeta con chip 300. El medio de procesador de tarjeta con chip 300 tienen acceso a un medio de memoria segura 302. El medio de memoria segura 302 contienen un programa 304 según una realización. Este programa 304 es operable para realizar la primera autenticación mutua criptográfica entre la tarjeta con chip de telecomunicaciones y el dispositivo terminal a través de la interfaz de lector de tarjeta con chip. El programa 304 es operable además para recibir un mensaje de configuración a través de la interfaz de lector de tarjeta con chip. El programa 304 es operable además para almacenar el mensaje de configuración en el medio de memoria segura 302 y el programa es operable para borrarse a sí mismo 304 del medio de memoria segura 302. El programa 304 también puede tener módulos criptográficos y/o pares de claves para descifrar el método de configuración en algunas realizaciones.

La Fig. 4 muestra la misma tarjeta con chip de telecomunicaciones 100 que se mostró en la Fig. 3. No obstante, en este ejemplo, el mensaje de configuración 400, 402, 404, 406, 408, 410 se ha escrito en el medio de memoria segura 302 y el programa 304 de la Fig. 3 ha sido eliminado. Se puede ver que en este ejemplo el medio de memoria segura 302 contiene información de abonado 400. La información de abonado como se usa en la presente memoria es información de datos que permite que el dispositivo de telefonía móvil se registre en la red de telecomunicaciones móviles celular digital. El medio de memoria segura 302 se muestra como conteniendo además números de teléfono 402. Los números de teléfono pueden ser, por ejemplo, números de abonado u otros números a los que el proveedor de la red de telecomunicaciones móviles digital desearía que el operador del dispositivo de telefonía móvil tuviera acceso cuando la tarjeta con chip de telecomunicaciones 100 se inserta en un dispositivo de telefonía móvil.

El medio de memoria segura 302 se muestra como que contiene además un sistema operativo 404. El medio de memoria segura 302 se muestra como que contiene además un anuncio 406 o datos de anuncio. El medio de memoria segura 302 se muestra además como que contiene una primera aplicación 408 y una segunda aplicación 410. Éstas son aplicaciones que se pueden ejecutar por el medio de procesador de tarjeta con chip 300 y realizan una función útil. Por ejemplo, la primera y segunda aplicaciones 408, 410 pueden usar tales cosas como los datos de anuncio 406 para mostrar o presentar anuncios a un operador del dispositivo de telefonía móvil. Los contenidos del medio de memoria segura 302 pueden variar. No todos los contenidos del medio de memoria segura 302 necesitan estar presentes.

La Fig. 5 muestra un sistema de actualización 500 según una realización de la invención. El sistema de actualización 500 comprende un dispositivo terminal 502 conectado opcionalmente a un servidor 504. El dispositivo terminal 502 comprende un medio de procesador de dispositivo terminal 506. El medio de procesador de dispositivo terminal está conectado a un lector de tarjeta con chip 507. El lector de tarjeta con chip 507 es operable para interconectar con una interfaz de lector de tarjeta con chip 102 de la tarjeta con chip de telecomunicaciones 100. El medio de procesador de dispositivo terminal 506 está conectado además a un medio de almacenamiento de ordenador 508 y a un medio de memoria de ordenador 510. El medio de procesador de dispositivo terminal 506 está conectado además a un medio de módulo criptográfico 512. El medio de módulo criptográfico 512 se pueden implementar como un módulo de software o un módulo de hardware y proporciona datos criptográficos para autenticar el dispositivo terminal y/o para proporcionar pares de claves para descifrado y cifrado de mensajes. Como se mencionó antes, el medio de módulo criptográfico 512 pueden ser un módulo de software almacenado en el almacenamiento de ordenador 508 o la memoria 510 o puede ser un testigo de seguridad individual tal como un módulo de plataforma informática de confianza o un dispositivo de hardware que almacena de manera segura datos biométricos y/o claves o pares de claves criptográficas.

El medio de procesador de dispositivo terminal 506 está conectado además a un medio de comunicación de red 514. El medio de comunicación de red 514 permite la formación de una conexión de red 516 al servidor 504. La conexión de red 516 es representativa y está destinada a representar una variedad de conexiones de red diferentes tales como Internet, Ethernet, o conexión de red de telecomunicaciones móviles digital. Por ejemplo, en algunos casos el dispositivo terminal 502 puede ser un teléfono inteligente o un teléfono inteligente especializado en lugar de ser simplemente un ordenador. El dispositivo terminal 502 puede ser en algunos casos un dispositivo informático móvil.

El medio de almacenamiento de ordenador 508 se muestra como que contiene un testigo de seguridad 518. El medio de almacenamiento de ordenador 508 se muestra además como que contiene una solicitud de mensaje de servidor criptográfico 520. El medio de almacenamiento de ordenador 508 se muestra además como que contiene un mensaje de servidor criptográfico 522. El medio de almacenamiento de ordenador 508 se muestra además como que contiene un mensaje de configuración 524 que se transferirá a través del lector de tarjeta con chip 507 a la tarjeta con chip de telecomunicaciones 100.

El medio de memoria de ordenador 510 se muestra como que contiene un módulo de control 526. El módulo de control 526 contiene un código ejecutable por procesador que permite al medio de procesador 506 comunicar con el servidor 504 y la tarjeta con chip de telecomunicaciones 100. El medio de memoria de ordenador 510 se muestra además como que contiene un módulo criptográfico 530. El módulo de autenticación mutua criptográfica 528 y el módulo criptográfico 530 contienen un código que permite que el medio de procesador 506 realice la autenticación y

cifrado y descifrado necesarios para transferir el mensaje de servidor criptográfico 522 y transformarlo en el mensaje de configuración 524 que se transmite entonces a la tarjeta con chip de telecomunicaciones 100.

El servidor 504 se muestra como que contiene un medio de procesador de servidor 540. El medio de procesador de servidor 540 está conectado a una interfaz de red 542 que permite la formación de la conexión de red 516 con el medio de comunicación de red 514. El medio de procesador 540 se muestra como que está conectado al medio de almacenamiento de ordenador 544 y al medio de memoria de ordenador 546. En este ejemplo, el medio de almacenamiento de ordenador 544 se muestra como que contiene el testigo de seguridad 518, la solicitud de mensaje de servidor criptográfico 520 y el mensaje de servidor criptográfico 522.

El medio de memoria de ordenador 546 se muestra como que contiene un módulo de control 548. El módulo de control contiene código que permite al medio de procesador 548 interactuar con el medio de terminal 502 para enviarle el mensaje de servidor criptográfico 522. El medio de memoria de ordenador 546 se muestra además como que contiene un módulo criptográfico 550 y un módulo de generación de mensaje de servidor criptográfico 522. Estos dos módulos permiten al procesador 540 responder al testigo de seguridad 518 y a la solicitud de mensaje de servidor criptográfico 520 generar el mensaje de servidor criptográfico 522.

La Fig. 6 muestra un ejemplo adicional de un sistema de actualización 600. El sistema de actualización en la Fig. 6 es similar al de la Fig. 5 y tiene muchos componentes equivalentes. Además, el dispositivo terminal 502 comprende una interfaz de usuario 602 y un sistema de medición biométrica 604. El sistema de medición biométrica 604 puede ser, por ejemplo, un lector de huella dactilar y/o un escáner de iris. La interfaz de usuario 602 y el sistema de medición biométrica 604 son capaces de comunicar con el medio de procesador 506.

El medio de almacenamiento de ordenador 508 se muestra como que contiene una medición biométrica 606 y una medición biométrica almacenada 608. La medición biométrica almacenada es opcional. En algunas realizaciones la medición biométrica almacenada 608 se puede comparar con la medición biométrica 606. Si la medición biométrica almacenada 608 no coincide con la medición biométrica 606 entonces el proceso de transferencia del mensaje de configuración 524 a la tarjeta con chip de telecomunicaciones 100 puede ser abortado o detenido. La medición biométrica almacenada 608 se puede almacenar de forma permanente o semipermanente en el almacenamiento 508 y/o se puede haber transferido desde el servidor 504 sobre la marcha.

El medio de memoria de ordenador 510 se muestra como que contiene un módulo de construcción de testigo criptográfico 610. Este módulo 610 no está presente en todas las realizaciones. El módulo de construcción de testigo criptográfico 610 construye el testigo de seguridad 518 usando al menos parcialmente la medición biométrica 606.

El sistema de servidor 504 también se modifica en este ejemplo. El medio de almacenamiento de ordenador 544 se muestra como que contiene una implementación de una base de datos biométrica 620 y una base de datos de abonados 630. Cuando un testigo de seguridad 518 comprende una medición biométrica, entonces la base de datos biométrica 620 se puede usar para identificar qué persona se identifica mediante la medición biométrica. El módulo de generación de mensaje de servidor criptográfico 552 puede usar la base de datos biométrica 620 y la base de datos de abonados 630 para construir el mensaje de servidor criptográfico 522.

En no todas las realizaciones estará presente el sistema de medición biométrica 604 y las mediciones biométricas asociadas y el testigo de seguridad. La interfaz de usuario 602 también se puede usar para introducir datos de usuario. Los datos de usuario 612 también se pueden usar por el módulo de construcción de testigo criptográfico 610 para construir el testigo de seguridad 518. Los datos de usuario 612 se muestran como que están almacenados en el almacenamiento de ordenador 508.

La Fig. 7 muestra un ejemplo adicional de un sistema de actualización 700. La realización mostrada en la Fig. 7 es similar a la mostrada en las Fig. 5 y 6. En este ejemplo hay un lector de tarjeta inteligente 702 que es operable para interconectar con una tarjeta inteligente 704. El lector de tarjeta inteligente 702 permite la recepción de un testigo de identidad 706 desde la tarjeta inteligente 704. El testigo de identidad 706 se muestra como que está almacenado en el medio de almacenamiento de ordenador 508. El módulo de construcción de testigo criptográfico 610 en este ejemplo usa el testigo de identidad 706 para construir al menos parcialmente el testigo de seguridad 518.

Los ejemplos mostrados en 5, 6 y 7 no son mutuamente exclusivos. Se entiende que las características de los ejemplos 5, 6 y 7 se pueden combinar entre sí.

Como se usa en la presente memoria, un CAD es un Dispositivo de Aceptación de Tarjeta. Como se usa en la presente memoria, GPRS es un Servicio General de Radio por Paquetes. Como se usa en la presente memoria, GSM es un Sistema Global para Comunicaciones Móviles. Como se usa en la presente memoria, HTTPS es un Protocolo de Transferencia de Hipertexto Seguro. Como se usa en la presente memoria, ICCID es un ID de Tarjeta de Circuito Integrado. Como se usa en la presente memoria, IP es un Protocolo de Internet. Como se usa en la presente memoria, PIN es un Número de Identificación Personal. Como se usa en la presente memoria, POS es un Punto de Venta. Como se usa en la presente memoria, PPP es un Protocolo Punto a Punto. Como se usa en la presente memoria, PSTN es una Red Telefónica Pública Conmutada. Como se usa en la presente memoria, SIM es un Módulo de Identidad de Abonado. Como se usa en la presente memoria, SRPS es un Sistema de Personalización Remota Segura. Como se usa en la presente memoria, SSL es una Capa de Conexiones Seguras.

Como se usa en la presente memoria, TLS es una Seguridad de Capa de Transporte. Como se usa en la presente memoria, TMS es un Sistema de Gestión de Terminal.

En la carrera de captura del mercado de Telecomunicaciones y competencia de vanguardia, existe una necesidad de aumentar el número de redes activas por los operadores, aumentar los perfiles soportados por los operadores y un sistema de gestión de la cadena de suministro mejorado para hacer llegar la SIM a los clientes a tiempo o estar disponible en todo momento.

Para estar en la carrera de esta competencia de vanguardia, los suministradores de SIM tienen que configurar el centro de personalización cerca del mercado de consumo para una gestión de la cadena de suministro mejorada. Esto añade una sobrecarga en el coste en el establecimiento de un centro de personalización, así como su gestión. Para superar este problema, existe la necesidad de una solución de bajo coste, segura y orientada al cliente.

Las realizaciones de la invención pueden proporcionar un sistema de actualización o un Sistema de Personalización Remota Segura (SRPS). El SRPS también se puede conocer como un sistema de actualización. El SRPS puede proporcionar los siguientes beneficios:

- Personalización e infraestructura de bajo coste.
- Responsabilidad de los ICCID perdidos, por lo tanto, reutilización de los ICCID perdidos.
- Soporte de múltiples operadores de datos e identificación también.
- Personalización remota usando comunicación basad en IP segura a través de GSM, GPRS, y PSTN.
- Comunicación segura entre la Tarjeta SIM y el Terminal (Punto de Personalización)

1. Arquitectura SRPS:

La arquitectura se puede diseñar teniendo en cuenta que los datos de personalización se pueden proporcionar por un proveedor de servicios de manera segura y los datos de personalización podrán residir en un servidor de base de datos.

La Fig. 8 muestra una ilustración funcional de un sistema de actualización 800. Se muestran múltiples ordenadores como que componen un servidor 504. Se muestran diversos medios de comunicaciones entre el servidor 504 y el dispositivo terminal 502. La comunicación entre el dispositivo terminal 502 se puede realizar usando una conexión segura SSL 802 a través de PSTN 802, GPRS 804 o GSM 806. Para las variantes GPRS 804 y GSM 806, se asigna 808 al dispositivo terminal una dirección IP dinámicamente.

SRPS puede construirse de diversas formas:

- Si el Proveedor de Servicios no quiere compartir sus datos con una empresa que personaliza las tarjetas SIM, una aplicación Web puede encaminar la solicitud desde el terminal al Servidor de Base de Datos del Proveedor de Servicios y los datos de respuesta se enviarán al terminal.

- La aplicación Web también puede residir en el Servidor del Proveedor de Servicios y el terminal puede solicitar directamente al Servidor del Proveedor de Servicios.

El dispositivo terminal y el servidor pueden comunicarse en una variedad de formas. Por ejemplo, usando:

- GPRS 804 pueden comunicarse en los siguientes pasos:

  - El terminal enviará una solicitud PPP al proveedor de servicios de red,

  - El proveedor de servicios de red asignará una IP Dinámica al terminal,

  - Ahora el terminal puede comunicar con seguridad (por ejemplo, a través de SSL como se describe a continuación) a través de Internet con el servidor.

- GSM 806 o PSTN 802 pueden comunicarse en los siguientes pasos:

  - El terminal enviará una solicitud PPP al servidor,

  - El servidor asignará una IP Dinámica al terminal,

  - Ahora el servidor Web y el terminal pueden comunicar con seguridad (por ejemplo, a través de SSL como se describe a continuación).

El software o la aplicación que ejecuta el dispositivo terminal se puede actualizar usando TMS.

1.1 Arquitectura de Componentes de Sistema:

1.1.1 Arquitectura de Comunicación:

Es posible que el operador de la red de telecomunicaciones digital y el proveedor del mensaje de configuración sean empresas diferentes. Para configurar correctamente la tarjeta con chip de telecomunicaciones puede ser beneficioso compartir datos entre las dos empresas.

Las características de tal sistema de compartición de datos pueden tener una o más de las siguientes características:

- El servidor y el servidor del proveedor de servicios pueden comunicarse sobre una red asegurada SSL.
- El servidor puede importar los datos de personalización desde el Servidor del Proveedor de Servicios.
- El Proveedor de Servicios puede acceder al informe de personalización a través de Registro y Contraseña desde el servidor directamente.

La Fig. 9 muestra un ejemplo de la conectividad posible entre el proveedor de tarjetas con chip de telecomunicaciones y diversos proveedores de servicios de telecomunicaciones. 504 representa el sistema de servidor de un proveedor de tarjetas con chip de telecomunicaciones. El sistema de servidor 504 proporciona el mensaje de servidor criptográfico usado por el dispositivo terminal para proporcionar el mensaje de configuración.

El servidor 900 representa los datos de una primera red de telecomunicaciones digital que proporciona una empresa. El servidor 902 representa los datos de una segunda red de telecomunicaciones digital que proporciona una empresa. El servidor 904 representa los datos de una tercera red de telecomunicaciones digital que proporciona una empresa. Los servidores 900, 902, 904 representan tres conjuntos diferentes de datos que se proporcionan al servidor 504 para personalizar las tarjetas con chip de telecomunicaciones.

El bloque 906 representa una primera red de telecomunicaciones digital que proporciona una empresa que se conecta al servidor 504 para acceder a datos. Esto, por ejemplo, puede ser para solicitar la personalización de una tarjeta con chip de telecomunicaciones. El bloque 908 representa una segunda red de telecomunicaciones digital que proporciona una empresa que se conecta al servidor 504 para acceder a datos. El bloque 910 representa una primera red de telecomunicaciones digital que proporciona una empresa que se conecta al servidor 504 para acceder a datos.

1.1.2 Arquitectura TMS

La Fig. 10 Ilustra una arquitectura TMS 1000 para actualizar software en el dispositivo terminal. Comprende componentes de servidor 504, componentes de red 516, y el dispositivo terminal. Se ilustran variantes de GPRS 1002, GSM 1004 y PSTN 1006.

El sistema TMS 1000 es un sistema basado en web disponible para actualizar la aplicación del terminal en la propia ubicación remota. La nueva versión de la aplicación de terminal publicada se puede actualizar por el servidor TMS en el terminal usando cualquier medio disponible, es decir, GSM 1002, GPRS 1004 y PSTN 1006. El TMS puede estar basado en una arquitectura cliente-servidor.

2. Componentes del sistema de actualización

2.1 El servidor o servidor web puede comprender:

- Un único punto de comunicación y
- Un mecanismo de solicitud y respuesta segura usando el protocolo HTTPS.
  - Recibir un Nº de Serie Único de Tarjeta desde el Terminal (es decir, Punto de Personalización).
  - Analizar sintácticamente un Nº de Serie Único.
  - Identificación del operador de telecomunicaciones usando el Nº de Serie Único.
  - Buscar y recuperar los elementos de datos en base a un Nº de Serie Único y un operador de telecomunicaciones identificado.
  - Enviar elementos de datos como respuesta al Terminal (es decir, Punto de personalización).
  - Actualizar detalles contra un Nº de Serie Único en la base de datos.
- Encaminamiento de la solicitud al servidor de base de datos específico del Operador de telecomunicaciones en caso de servidor de base de datos propiedad de los Operadores de telecomunicaciones.

- Emisión de Terminal y su autenticación.

2.2 Servidor de base de datos

- Almacenamiento seguro.
- Accesibilidad segura.
- Almacenar elementos de datos de personalización y perfil de operador de telecomunicaciones único o múltiple.
- Interfaz abstracta para diferentes operadores de telecomunicaciones.

2.3 Terminal

2.3.1 Hay varios métodos diferentes en los cuales un dispositivo terminal puede verificar al usuario:

- Huella dactilar en el Terminal: Almacenar la huella dactilar del usuario en el terminal y siempre que se inicie el terminal, pedirá la verificación de la huella dactilar del usuario.
- Huella dactilar en la Tarjeta Inteligente: una Tarjeta Inteligente se puede emitir a un usuario con la huella dactilar en la tarjeta y el terminal le pedirá la tarjeta siempre que se inicie el terminal.
- Autenticación en el servidor: La huella dactilar del usuario se almacenará en el servidor y en el Terminal/Tarjeta inteligente. Siempre que un usuario intente registrarse en la aplicación de terminal, la primera verificación se hará en el terminal y entonces el terminal enviará detalles de la huella dactilar al servidor y se autenticará en el servidor también.
- Verificación del PIN: El PIN se puede almacenar en el terminal/Tarjeta Inteligente y siempre que se inicie el terminal, pedirá la verificación del PIN.

2.3.2 Protocolo de comunicación:

En algunas realizaciones, se puede usar un protocolo de comunicación como se muestra en la Fig. 11. La Fig. 11 ilustra un método de un protocolo de comunicación 1100 entre un dispositivo terminal 502 y un servidor 504. En el ejemplo mostrado en la Fig. 11 el dispositivo terminal 502 y el servidor 504 pueden intercambiar datos 1102 usando GSM, GPRS o PSTN. En el paso 1104, el dispositivo terminal 502 inicia 1104 la comunicación con el servidor 504. A continuación, en el paso 1106, el servidor 504 envía 1106 al terminal 502 un mensaje de acuse de recibo OK. En el paso 1108, el dispositivo terminal 502 solicita 1108 datos de personalización y un número de serie para la tarjeta con chip de telecomunicaciones desde el servidor 504. En el paso 1110, el servidor 504 envía al dispositivo terminal 502 detalles de personalización para la tarjeta con chip de telecomunicaciones. Los detalles de personalización son un ejemplo de un mensaje de servidor criptográfico. El dispositivo terminal 502 usa los detalles de personalización para enviar el mensaje de configuración a la tarjeta con chip de telecomunicaciones. Después de completar esto, el dispositivo terminal 502 envía 1112 un mensaje de acuse de recibo al servidor 504.

2.3.3 Modo de Personalización:

2.3.3.1 En una realización se pueden formar los siguientes pasos para personalización en línea: Insertar la tarjeta SIM en el terminal, conectar con el servidor usando cualquier medio de comunicación disponible (GSM/GPRS/PSTN), descargar elementos de datos de personalización específicos del operador de telecomunicaciones según el perfil soportado por la tarjeta SIM, realizar la personalización de la tarjeta SIM, y enviar acuse de recibo al servidor.

3. Atomicidad de Transacción

Las realizaciones pueden tener una o más de las siguientes características para asegurar que solamente se realizan actualizaciones completas de una tarjeta con chip de telecomunicaciones:

- Si se envió una solicitud por un dispositivo terminal y no se recibió ninguna respuesta de un Servidor, se mostrará en el terminal un mensaje de “TIEMPO DE ESPERA”.
- Si se envió una solicitud por el terminal con un “número de serie” pero no se encuentra ningún registro correspondiente por el servidor, se mostrará en el terminal un mensaje “NÚMERO DE SERIE INVÁLIDO” o un mensaje equivalente.
- El dispositivo terminal puede comprobar la integridad de los datos recibidos desde el servidor.

- Si el dispositivo terminal no es capaz de actualizar un archivo particular en la tarjeta SIM, el dispositivo terminal puede mostrar el error de fallo de personalización y enviará un código de error (devuelto por la tarjeta en el momento de la personalización) al Servidor.

- Si la tarjeta con chip de telecomunicaciones se actualiza o no con éxito, pero el terminal no pudo enviar los detalles al servidor debido a un fallo de conexión, el terminal almacenará los detalles localmente y siempre que se conecte al servidor, los datos no enviados se registrarán y el dispositivo terminal enviará los registros al servidor.

4. Seguridad

4.1 Seguridad de Comunicación

4.1.1 Terminal y Tarjeta

Un aspecto importante de cualquier sistema de personalización o sistema de actualización remoto es cómo asegurar la comunicación entre el CAD (Dispositivo de Aceptación de Tarjeta) y la Tarjeta Inteligente/SIM. Esta sección explica algunas debilidades de la comunicación SIM y CAD y posibles contramedidas.

4.1.1.1 Violaciones de seguridad en Tarjetas Inteligentes

Una Tarjeta Inteligente y un Dispositivo de Aceptación de Tarjeta (CAD) pueden comunicarse a través de medios de paquetes de datos pequeños llamados APDU (Unidades de Datos de Protocolo de Aplicaciones). Las siguientes características de esta interacción hacen más difícil a terceros atacar el sistema con éxito:

- Velocidad de bit pequeña (9600 bits por segundo) usando una línea de transmisión bidireccional en serie (estándar ISO 7816/3),

- modo semidúplex para enviar la información (los datos solamente viajan en una dirección a la vez)

- La comunicación sigue un protocolo sofisticado, descrito a continuación.

- No obstante, cada dispositivo externo que comunica con la tarjeta la hacen más vulnerable de atacar a través del enlace de comunicación.

También hay problemas de seguridad relacionados con el riesgo de que la comunicación entre estos componentes de sistema, se pueda monitorizar o escanear por piratas informáticos. Sería beneficioso desarrollar métodos que mejoren la seguridad de los componentes individuales y el sistema de actualización completo.

El uso de una tarjeta inteligente para asegurar datos seguros personales se podrá beneficiar por algoritmos criptográficos y protocolos de seguridad realzados o mejorados que pueden ser más rápidos de ejecutar y más pequeños en tamaño mirando la limitación de espacio en la tarjeta inteligente.

4.1.1.2 Mecanismo de Seguridad

La Tarjeta Inteligente y el CAD usan un protocolo de autenticación activa mutua para identificarse entre sí. La tarjeta genera un número aleatorio y lo envía al CAD, que cifra el número con una clave de cifrado compartida antes de devolverlo a la tarjeta. La tarjeta entonces compara el resultado devuelto con su propio cifrado. La pareja puede entonces realizar la operación a la inversa.

Una vez que se establece la comunicación, cada mensaje entre la pareja se verifica a través de un código de autenticación de mensaje. Este es un número que se calcula en base a los propios datos, una clave de cifrado y un número aleatorio. Si los datos se han alterado (por cualquier razón, incluyendo errores de transmisión) se debe retransmitir el mensaje. Alternativamente, si el chip tiene suficiente memoria y potencia de procesamiento, los datos se pueden verificar a través de una firma digital.

La miniaplicación seleccionada o la activa y el programa de aplicación de cliente (programa en el terminal, que invoca la aplicación de miniaplicación de tarjeta) a través del cual está comunicando la miniaplicación, se deberían ocupar de estos intercambios de datos.

La Fig. 12 muestra un diagrama de flujo que ilustra los componentes usados para realizar un método de una miniaplicación que procesa los comandos de actualización que se reciben por un terminal de forma cifrada y luego se pasan a la miniaplicación para descifrado y procesados adicional por un Sistema Operativo de tarjeta. Primero en el bloque 1202 los comandos recibidos desde el servidor por el terminal como un archivo o una secuencia de comandos. A continuación, en el bloque 1204 una aplicación en el terminal prepara el comando especial específico de la tarjeta con chip para ser enviado a un CAD (Dispositivo de aceptación de tarjeta).

El bloque 1206 procesa los comandos preparados en el bloque 1204. El Dispositivo de aceptación de tarjetas (CAD) es básicamente un dispositivo de interfaz de tarjeta que realiza la lectura y/o escritura en la tarjeta sobre la base de

las solicitudes recibidas desde el terminal. A continuación, en el bloque 1208 un conjunto de comandos especiales específicos de tarjeta que se destinan solamente para ese tipo de tarjeta específica.

El bloque 1210 representa una miniaplicación pequeña de autodestrucción que está descifrando los comandos cifrados antes de pasar estos comandos al sistema operativo. La miniaplicación se destruirá, o borrará, a sí misma al final de este proceso. El bloque 1212 representa el Sistema Operativo de Tarjeta que pasó los comandos por la miniaplicación de autodestrucción del bloque 1210.

La Fig. 13 ilustra un protocolo de comunicación 1300 entre un dispositivo terminal 1302 y una tarjeta inteligente 1304. La tarjeta inteligente 1304 puede ser una tarjeta con chip de telecomunicaciones. El dispositivo terminal 1302 tiene una aplicación que envía mensajes APDU a través de un lector de tarjeta con chip 507 a la interfaz de lector de tarjeta con chip 102. El medio de procesador 300 funciona como un procesador APDU para codificar y decodificar mensajes APDU.

4.1.1.3 Breve descripción de la Aplicación

La aplicación soportará la actualización del archivo de registro y binario con datos cifrados en un entorno seguro en la tarjeta. La aplicación tomará la Clave Maestra como entrada en el momento de la instalación, luego genera la clave individual de Tarjeta que se usa para descifrar el valor cifrado en los comandos APDU de miniaplicación.

Esta aplicación describe el formato APDU para actualizar el archivo de registro y el archivo transparente. También define el algoritmo de generación de claves únicas que se usa por la aplicación para descifrar el valor cifrado. El mismo algoritmo se debe usar por la aplicación fuera de la tarjeta para cifrar los datos para el comando APDU.

La aplicación de Miniaplicación de Personalización Cifrada se puede dividir en los siguientes módulos:

1) Generación de Clave de Cifrado

2) Comandos APDU para Actualización Binaria y Actualización de Registro

3) Comando APDU para desactivar la miniaplicación.

4) Procesamiento de comando APDU.

4.1.1.4 Generación de Clave

Para la Miniaplicación de Personalización Cifrada, el valor de actualización viene en formato cifrado. El cifrado se puede hacer usando un formato único. La miniaplicación puede generar una clave única para cada tarjeta para descifrar el valor cifrado o el mensaje de configuración.

La Fig. 14 muestra un diagrama de bloques 1400 que ilustra un método de generación de una Clave Individual de Tarjeta (CIK). La CIK es la clave utilizada por la tarjeta con chip de telecomunicaciones para descifrar el mensaje de configuración. En el paso 1402, la miniaplicación recibe como entrada una Clave Maestra durante la instalación. En el paso 1404 se utiliza un algoritmo de generación de clave para producir la CIK 1406.

4.1.1.5 Procesamiento de Comando APDU

Cuando la Miniaplicación recibe el comando APDU, comprueba la integridad del comando. Si es válido entonces procesa los datos. La miniaplicación puede ser operable para realizar las siguientes acciones:

- Primero descifra la parte de datos cifrados.
- Segundo, selecciona los archivos en el mismo orden en que los recibe.
- Para actualización de comando binario toma el desplazamiento a partir del parámetro P1 P2 en el comando APDU y ejecuta el comando binario de actualización.
- Para actualización del comando de registro toma el número de registro a partir del parámetro P1 en el comando APDU y ejecuta el comando de registro de actualización.

4.1.2 Dispositivo Terminal y Servidor

El dispositivo terminal puede usar una Capa de Conexiones Seguras (SSL) para comunicarse con el servidor. SSL protege los datos transferidos sobre el protocolo de transferencia de hipertexto (http) usando el cifrado habilitado por el Certificado SSL de un servidor.

4.1.2.1 El uso del protocolo SSL/TLS puede ser ventajoso debido a que:

- El uso de otros protocolos de seguridad en lugar de TLS/SSL está prohibido en el ámbito del acuerdo de Programa de Seguridad de Terminal POS (PTS), debido a la especificidad de la plataforma, el perímetro de

la certificación PTS se limita al uso del protocolo de seguridad: SSL v3 o TLS 1.0 suministrado por SAGEM Monetel.

- Si los desarrolladores de terceros quieren añadir un nuevo protocolo de seguridad, tendrán que solicitar una certificación PTS adicional. Esta aprobación adicional se debe tener en cuenta por los desarrolladores de terceros.

4.1.3 Servidor y Servidor de Proveedor de Servicios

Para poder comunicar un servidor que proporciona el mensaje de configuración y un servidor que pertenece a la red de telecomunicaciones móviles digital, un protocolo de comunicación SSL se puede usar para asegurar el enlace de comunicación entre el Servidor y Servidor de Proveedor de Servicios.

4.2 Seguridad de Datos

4.2.1 La Seguridad de Datos en el Servidor se puede proporcionar de las siguientes formas:

- Se puede usar un Cortafuegos entre el Servidor y la red que filtrará la información entrante o saliente.
- El Usuario Autenticado puede obtener acceso a la base de datos o a los objetos del esquema de base de datos y realizará solamente acciones autorizadas.

4.2.2 La Seguridad de Datos en el Terminal se puede proporcionar de las siguientes formas:

- Idealmente, el terminal se puede conectar durante el proceso de personalización. Pero si ocurre un fallo de comunicación entonces el estado de personalización de la tarjeta se almacenará en el terminal localmente durante un período de tiempo temporal.
- Los datos almacenados en el terminal están asegurados debido a que los datos permanecerán invisibles al mundo exterior.

4.2.3 La Seguridad de Datos en la Tarjeta se puede proporcionar de las siguientes formas:

- Una vez que la tarjeta está personalizada, el acceso a la tarjeta con chip de telecomunicaciones se bloquea de forma que no se permitirá ningún otro comando distinto del comando específico GSM.
- Los datos como las claves de autenticación y el PIN se almacenan en el área segura de la tarjeta SIM, los cuales son accesibles por las APDU.

4.3 Seguridad física de terminal y de tarjeta:

- Puede ser responsabilidad del usuario del terminal mantener el terminal y la tarjeta físicamente asegurados.
- La aplicación se puede asegurar con el método de seguridad proporcionado (huella dactilar o contraseña). Así que solamente el usuario autenticado del terminal podría acceder a la aplicación y personalizar la tarjeta.

5. Gestión de Recuperación de Desastres

5.1 Servidor de base de datos:

La recuperación de desastres es el proceso, las políticas y los procedimientos relacionados con la preparación para la recuperación o la continuación de la infraestructura tecnológica crítica para una organización después de un desastre natural o inducido por el hombre. Para minimizar el riesgo de desastres, se pueden tomar las siguientes medidas:

- Las copias de seguridad se deberían realizar usando otro disco físico según la política de copias de seguridad decidida.
- Replicar la fecha del servidor en otro servidor de base de datos, que supera la necesidad de restaurar los datos.
- Fuente de alimentación ininterrumpida (UPS) y/o generador de reserva para mantener los sistemas en marcha en caso de un fallo de energía.
- Desplegar dispositivos de prevención de incendios tales como alarmas y extintores de incendios.
- Usar software antivirus y otras medidas de seguridad en dispositivos informáticos u ordenadores.

5.2 Terminal

Si el dispositivo terminal llega a ser no funcional debido a cualquier razón, entonces el terminal se puede sustituir con un nuevo terminal y el terminal existente se puede enviar para su mantenimiento.

6. Apéndice I

6.1 Capa de Conexiones Seguras (SSL): Cómo funciona

La tecnología de Capa de Conexiones Seguras (SSL) protege el sitio Web y facilita a los visitantes del sitio Web confiar de tres formas esenciales:

- Un certificado SSL permite el cifrado de información sensible durante las transacciones en línea.
- Cada certificado SSL contiene información única, autenticada acerca del propietario del certificado.
- Una Autoridad de Certificación verifica la identidad del propietario del certificado cuando se emite.

6.1.1 Cómo funciona el cifrado:

- Un Certificado SSL establece un canal de comunicación privado que permite el cifrado de los datos durante la transmisión. El cifrado aleatoriza los datos, esencialmente creando un sobre para la privacidad del mensaje.
- Cada Certificado SSL consta de una clave pública y una clave privada. La clave pública se usa para cifrar información y la clave privada se usa para descifrarla.
- Cuando un navegador Web apunta a un dominio seguro, un inicio de diálogo de la Capa de Conexiones Seguras autentica el servidor (sitio Web) y el cliente (explorador Web). Se establece un método de cifrado con una clave de sesión única y se puede comenzar una transmisión segura.

6.1.2 Certificados:

Un certificado es una declaración firmada digitalmente desde una entidad que certifica que información acerca de otra entidad es verdadera. Un certificado es un conjunto de información, firmado por una entidad emisora.

Los algoritmos de firma se pueden basar en criptografía de clave asimétrica (generalmente RSA). La entidad emisora firma cifrando el conjunto de información con su clave privada (conocida solamente por sí misma). Las otras entidades pueden verificar la firma descifrando el conjunto de información con la clave pública del emisor.

SSL usa el principio de certificado para operar la autenticación de las entidades (cliente y servidor). Estos certificados se codifican según el estándar X509. Este estándar define qué información puede contener un certificado, y describe al formato de datos cómo anotarlo. Todos los certificados X.509 contienen los siguientes datos, además de la firma: Versión, Número de Serie, Identificador de Algoritmo de Firma, Nombre de Emisor, Período de Validez, Nombre del Sujeto, e Información de Clave Pública del Sujeto.

6.1.3 Inicio de diálogo SSL.

La Fig. 15 ilustra un método 1500 de un inicio de diálogo SSL entre un cliente SSL 1502 y un servidor SSL 1504:

- El cliente SSL 1502 envía 1506 un mensaje “hola de cliente” que enumera información criptográfica tal como la versión SSL y, en el orden de preferencia del cliente, los Conjuntos de Cifrado soportados por el cliente. El mensaje también contiene una cadena de bytes aleatoria que se usa en cálculos posteriores. El protocolo SSL permite que el “hola de cliente” incluya los métodos de compresión de datos soportados por el cliente, pero las implementaciones SSL actuales normalmente no incluyen esta disposición.
- El servidor SSL 1504 responde 1508 con un mensaje de “hola de servidor” que contiene el Conjunto de Cifrado elegido por el servidor a partir de la lista proporcionada por el cliente SSL 1502, el ID de sesión y otra cadena de bytes aleatoria. El servidor SSL 1504 también envía su certificado digital. Si el servidor requiere un certificado digital para la autenticación del cliente, el servidor envía una “solicitud de certificado de cliente” que incluye una lista de los tipos de certificados soportados y los Nombres Distinguidos de Autoridades de Certificación (CA) aceptables.
- El cliente SSL 1502 verifica 1510 la firma digital en el certificado digital del servidor SSL y comprueba que el Conjunto de Cifrado elegido por el servidor 1504 es aceptable.
- El cliente SSL 1502 envía 1512 la cadena de bytes aleatoria que permite que tanto el cliente 1502 como el servidor 1504 calculen la clave secreta a ser usada para cifrar los datos de mensaje posteriores. La propia cadena de bytes aleatoria se cifra con la clave pública del servidor.

- Si el servidor SSL 1504 envía una “solicitud de certificado de cliente”, el cliente SSL 1502 envía 1514 una cadena de bytes aleatoria cifrada con la clave privada de cliente, junto con el certificado digital de cliente, o una “alerta de sin certificado digital”. Esta alerta es solamente una advertencia, pero con algunas implementaciones el inicio de diálogo falla si la autenticación del cliente es obligatoria.
- El servidor SSL 1504 verifica 1516 la firma en el certificado de cliente.
- El cliente SSL 1502 envía 1518 al servidor SSL 1504 un mensaje “finalizado”, que se cifra con la clave secreta, indicando que la parte de cliente del inicio de diálogo está completa.
- El servidor SSL 1504 envía 1520 al cliente SSL 1502 un mensaje “finalizado”, que se cifra con la clave secreta, indicando que la parte de servidor del inicio de diálogo está completa.
- Durante la duración de la sesión SSL, el servidor SSL 1504 y el cliente SSL 1502 ahora pueden intercambiar 1522 mensajes que están cifrados simétricamente con la clave secreta compartida.

6.1.4 Requisitos de base para SSL:

Para el terminal, la estructura PKI impone algunos requisitos para la definición del perfil SSL, principalmente para que se cumpla el acuerdo de Programa PTS:

- Solamente los algoritmos: 3DES y AES se deben usar para el cifrado de la sesión SSL/TLS
- La longitud mínima de las claves 3DES o AES debe ser de al menos 128 bits.
- El método de autenticación debe usar algoritmos RSA o DSS. La longitud de las claves públicas debe ser al menos 1024.
- Solamente se debe usar el algoritmo de comprobación aleatoria SHA-1. El uso de MD5 está prohibido.

Se recomienda autenticación mutua pero no es obligatoria.

Lista de números de referencia

100	tarjeta con chip de telecomunicaciones
102	interfaz de lector de tarjeta con chip
104	dispositivo de telefonía móvil
106	lector de tarjeta con chip
107	red de telecomunicaciones móviles celular digital
108	enlace radio
110	estación base
112	controlador de red radio
114	red de telecomunicaciones
300	medio de procesador de tarjeta con chip
302	medio de memoria segura
304	programa
400	información de abonado
402	números de teléfono
404	sistema operativo
406	anuncio
408	primera aplicación
410	segunda aplicación
500	sistema de actualización

502 dispositivo terminal

504 servidor

506 medio de procesador de dispositivo terminal

507 lector de tarjeta con chip

508 medio de almacenamiento de ordenador

510 medio de memoria de ordenador

512 medio de módulo criptográfico

514 medio de comunicaciones de red

516 conexión de red

518 testigo de seguridad

520 solicitud de mensaje de servidor criptográfico

522 mensaje de servidor criptográfico

524 mensaje de configuración

526 módulo de control

528 módulo de autenticación mutua criptográfica

530 módulo criptográfico

540 medio de procesador de servidor

542 medio de comunicaciones de red

544 medio de almacenamiento de ordenador

546 medio de memoria de ordenador

548 módulo de control

550 módulo criptográfico

552 módulo de generación de mensaje de servidor criptográfico

600 sistema de actualización

602 interfaz de usuario

604 sistema de medición biométrica

606 medición biométrica

608 medición biométrica almacenada

610 módulo de construcción de testigo criptográfico

612 datos de usuario

620 base de datos biométrica

630 base de datos de abonado

700 sistema de actualización

702 lector de tarjeta inteligente

704 tarjeta inteligente

706 testigo de identidad

800 sistema de actualización

802 PSTN

804 GPRS

806 GSM

808 asignación IP dinámica

900 servidor

902 servidor

904 servidor

906 acceso a servidor

908 acceso a servidor

910 acceso a servidor

1000 sistema de gestión de telecomunicaciones

1002 GPRS

1004 GSM

1006 PSTN

1100 protocolo de comunicación

1200 sistema de actualización

1202 secuencia de comandos

1204 aplicación de terminal

1206 CAD

1208 CMD

1210 aplicación de intérprete

1212 sistema operativo de tarjeta

1300 protocolo de comunicación

1400 método de generación de claves

1500 método de inicio de diálogo SSL

1502 cliente SSL

1504 servidor SSL

REIVINDICACIONES

1. Una tarjeta con chip de telecomunicaciones (100) para permitir el registro de un dispositivo de telefonía móvil (104) en una red de telecomunicaciones móviles celular digital (107) que comprende:

- una interfaz de lector de tarjeta con chip (102) adaptada para permitir comunicaciones entre la tarjeta con chip de telecomunicaciones y el dispositivo de telefonía móvil;

- un medio de procesador de tarjeta con chip (300);

- un medio de memoria segura (302) para almacenar programas para ejecución por el medio de procesador de tarjeta con chip; y

- un programa (304) almacenado en el medio de memoria segura que comprende instrucciones legibles por máquina ejecutables por el medio de procesador de tarjeta con chip; en donde la ejecución del programa hace al medio de procesador de tarjeta con chip realizar los pasos de:

- realizar (200) una primera autenticación mutua criptográfica entre la tarjeta con chip de telecomunicaciones y un dispositivo terminal (502) a través de la interfaz de lector de tarjeta con chip, en donde el dispositivo terminal tiene un lector de tarjeta con chip (507) operable para conectarse a la interfaz de lector de tarjeta con chip;

- recibir (214) un mensaje de configuración (400, 402, 404, 406, 408, 410, 524) a través de la interfaz de lector de tarjeta con chip;

- almacenar (216) el mensaje de configuración en el medio de memoria segura;

- borrar (218) el programa del medio de memoria segura, de manera que la tarjeta con chip de telecomunicaciones (100) se puede modificar solamente una vez.

2. La tarjeta con chip de telecomunicaciones de la reivindicación 1, en donde la ejecución de las instrucciones hace además al medio de procesador de tarjeta con chip realizar cualquiera de los siguientes:

realizar una autenticación MAC del mensaje de configuración, verificar una firma digital del mensaje de configuración, descifrar el mensaje de configuración, y combinaciones de los mismos.

3. La tarjeta con chip de telecomunicaciones de la reivindicación 2 o 3, en donde el mensaje de configuración es cualquiera de los siguientes: un conjunto de números de teléfono (402), información de abonado (400), un sistema operativo (404), datos de anuncio (406), una aplicación (408, 410), y combinaciones de los mismos.

4. La tarjeta con chip de telecomunicaciones de la reivindicación 1, 2 o 3, en donde la ejecución de las instrucciones hace al medio de procesador de tarjeta con chip borrar el medio de memoria segura antes de almacenar el mensaje de configuración en el medio de memoria segura.

5. Un sistema de actualización (500, 600, 700, 800) con una tarjeta con chip de telecomunicaciones (100) según cualquiera de las reivindicaciones precedentes para modificar la tarjeta con chip de telecomunicaciones (100), en donde el sistema de actualización comprende un dispositivo terminal (502), en donde el dispositivo terminal comprende:

- un lector de tarjeta con chip (507) operable para recibir la tarjeta con chip de telecomunicaciones y para intercambio de datos con la interfaz de lector de tarjeta con chip (102);

- un medio de procesador de dispositivo terminal (506);

- un medio de memoria terminal (510) para almacenar un programa de medio de terminal, en donde la ejecución del programa de medio de terminal hace al medio de procesador terminal:

- realizar (200) una primera autenticación mutua criptográfica entre el dispositivo terminal y la tarjeta con chip de telecomunicaciones a través de la interfaz de lector de tarjeta con chip;

- realizar (202) una segunda autenticación mutua criptográfica entre el dispositivo terminal y un servidor (504);

- enviar (204) un testigo de seguridad criptográfico (518) a un servidor;

- solicitar (206) un mensaje de servidor criptográfico (522) desde el servidor;

- recibir (208) el mensaje de servidor criptográfico desde el servidor;

- descifrar (210) el mensaje de servidor criptográfico usando una clave criptográfica (530);

- construir (212) un mensaje de configuración (524) usando el mensaje de servidor criptográfico descifrado;

- enviar (214) el mensaje de configuración a la tarjeta con chip de telecomunicaciones a través de la interfaz de lector de tarjeta con chip.

6. El sistema de actualización de la reivindicación 5, en donde el dispositivo terminal comprende un lector de huella dactilar (604) para escanear una huella dactilar (606) de un operador.

7. El sistema de actualización de la reivindicación 6, en donde el dispositivo terminal comprende además un registro de huella dactilar (608) almacenado en el medio de memoria de dispositivo terminal, en donde la ejecución del programa de medio de terminal hace además al procesador del terminal verificar la huella dactilar comparando la huella dactilar con el registro de huella dactilar, y en donde la ejecución del programa de medio de terminal hace al medio de procesador de terminal abortar la solicitud del mensaje de servidor criptográfico a menos que se verifique la huella dactilar.

8. El sistema de actualización de la reivindicación 6 o 7, en donde el testigo de seguridad comprende la huella dactilar.

9. El sistema de actualización de cualquiera de las reivindicaciones 5 a 8, en donde el sistema de actualización comprende además un lector de tarjeta inteligente (702) operable para interconectar con una tarjeta inteligente (704), en donde la ejecución del programa de medio de terminal hace además al medio de procesador de terminal:

- realizar una validación criptográfica de la tarjeta inteligente, y

- abortar la solicitud del mensaje de servidor criptográfico a menos que se verifique la huella dactilar.

10. El sistema de actualización de la reivindicación 9, en donde la tarjeta inteligente comprende una memoria de tarjeta inteligente que contiene un testigo de identidad (706); en donde el testigo de identidad comprende cualquiera de los siguientes: datos de huella dactilar almacenados, datos biométricos, datos de escaneado de iris, datos de autenticación criptográfica, y combinaciones de los mismos; en donde la ejecución del programa de medio de terminal hace al procesador de medio de terminal recuperar el testigo de identidad de la memoria de tarjeta inteligente a través del lector de tarjeta inteligente, en donde el testigo de seguridad comprende el testigo de identidad.

11. El sistema de actualización de cualquiera de las reivindicaciones 5 a 10, en donde el dispositivo terminal comprende además una interfaz de usuario (602), en donde la ejecución de las instrucciones hace además al procesador de terminal recibir datos de usuario (612) desde la interfaz de usuario, en donde el testigo de seguridad comprende los datos de usuario.

12. El sistema de actualización de cualquiera de las reivindicaciones 5 a 11, en donde el sistema de actualización comprende el servidor.

13. Un método de configuración de una tarjeta con chip de telecomunicaciones (100) usando un sistema de actualización (500, 600, 700, 800), en donde la tarjeta con chip de telecomunicaciones comprende una interfaz de lector de tarjeta con chip (102) adaptada para permitir comunicaciones entre la tarjeta con chip de telecomunicaciones y un dispositivo de telefonía móvil, en donde la tarjeta con chip de telecomunicaciones comprende además un medio de procesador de tarjeta con chip (300), en donde la tarjeta con chip de telecomunicaciones comprende además un medio de memoria segura (302) para almacenar programas para ejecución por el medio de procesador de tarjeta con chip, en donde la tarjeta con chip de telecomunicaciones además comprende un programa (304) almacenado en el medio seguro que comprende instrucciones legibles por máquina ejecutables por el medio de procesador de tarjeta con chip, en donde el sistema de actualización comprende un dispositivo terminal (502), en donde el dispositivo terminal comprende un lector de tarjeta con chip (507) operable para recibir la tarjeta con chip de telecomunicaciones y para intercambiar datos con la interfaz de lector de tarjeta con chip, en donde el método comprende los pasos de:

- realizar (200) una primera autenticación mutua criptográfica entre el dispositivo terminal y la tarjeta con chip de telecomunicaciones usando la interfaz de lector de tarjeta con chip;

- realizar (202) una segunda autenticación mutua criptográfica entre el dispositivo terminal y un servidor;

- enviar (204) un testigo de seguridad criptográfico (518) desde el dispositivo terminal al servidor;

- enviar (206) una solicitud de mensaje de servidor criptográfico (520) desde el dispositivo terminal al servidor;

- enviar (208) un mensaje de servidor criptográfico (522) desde el servidor al dispositivo terminal;

- descifrar (210) el mensaje de servidor criptográfico usando una clave criptográfica (530);

- construir (212) un mensaje de configuración (524) usando el mensaje de servidor criptográfico descifrado;

- enviar (214) el mensaje de configuración desde el dispositivo terminal a la tarjeta con chip de telecomunicaciones;

- almacenar (216) el mensaje de configuración en el medio de memoria segura; y

- borrar (218) el programa del medio de memoria, de manera que la tarjeta con chip de telecomunicaciones (100) se pueda modificar solamente una vez.

14. El método de la reivindicación 13, en donde el método comprende además identificar un abonado usando el testigo de seguridad criptográfico.

15. El método de la reivindicación 14, en donde el testigo de seguridad comprende un identificador biométrico, y en donde el abonado se identifica comparando el identificador biométrico con una base de datos biométrica.

Fig. 1

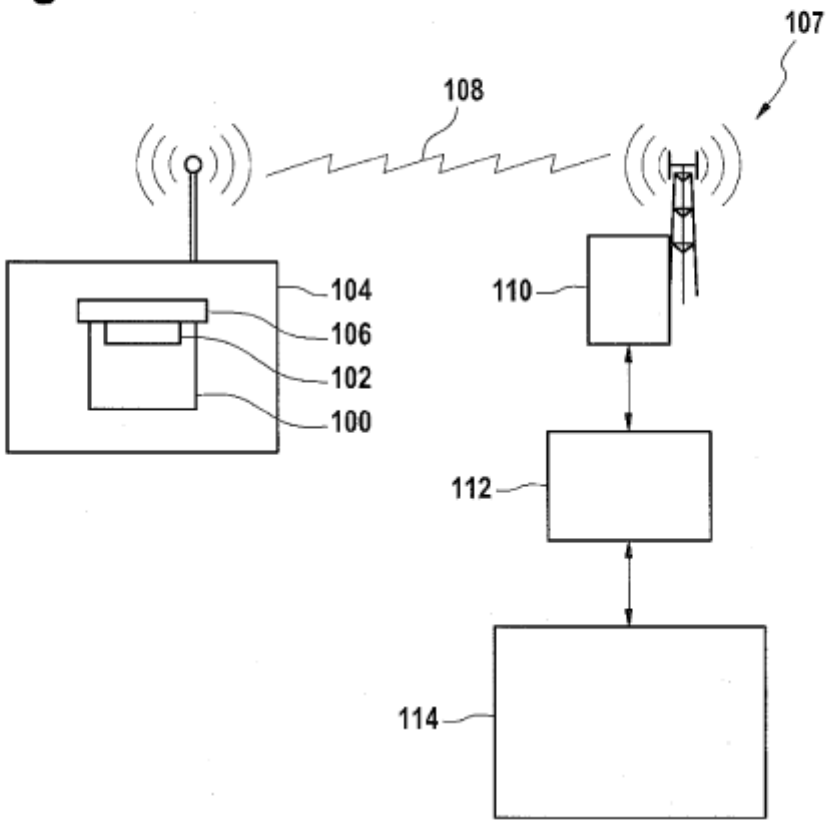


Fig. 2

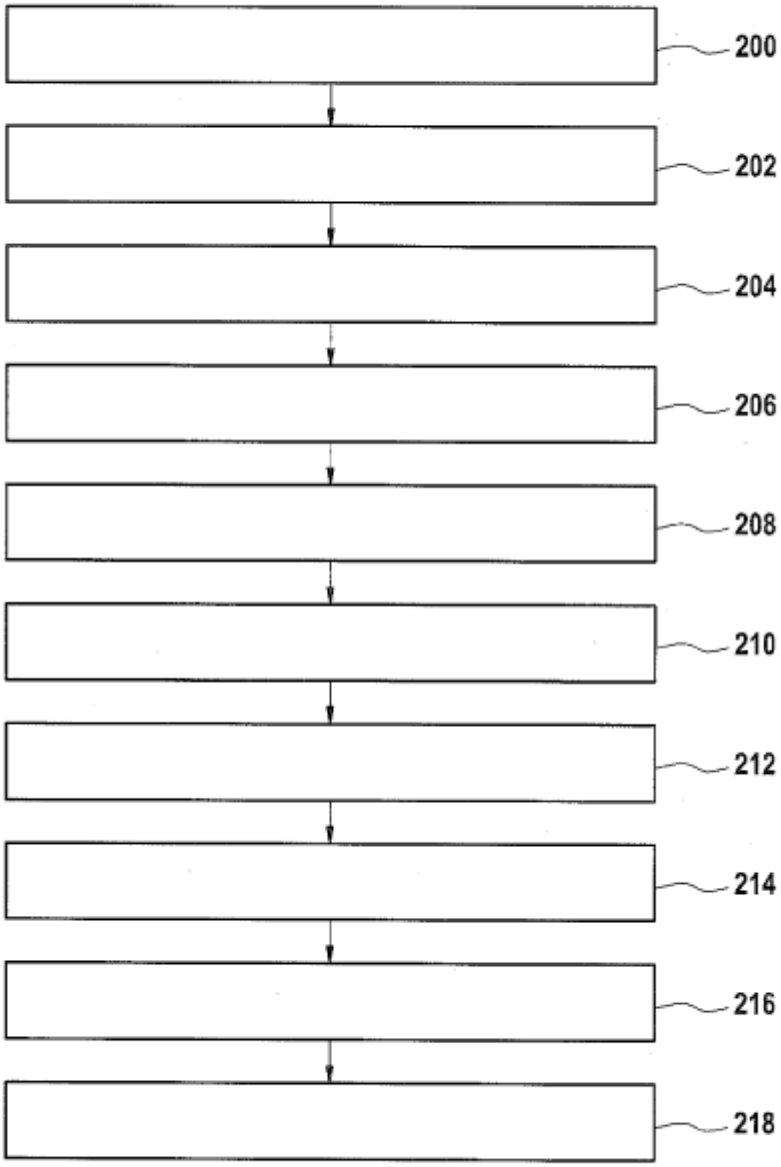


Fig. 3

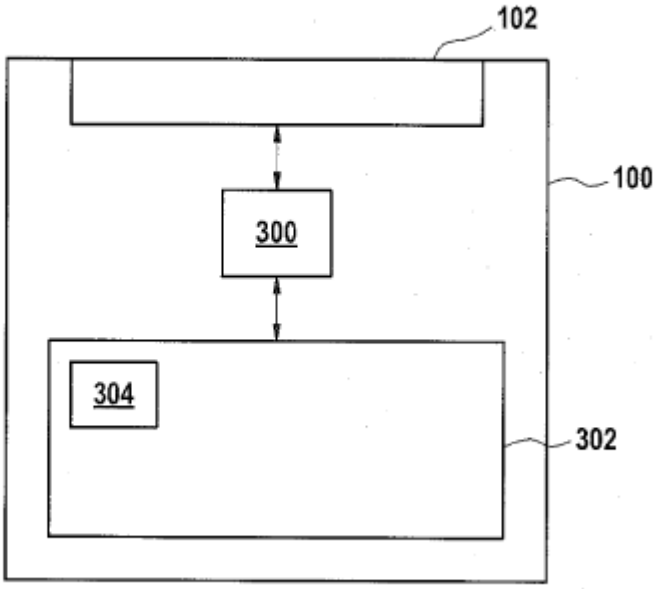


Fig. 4

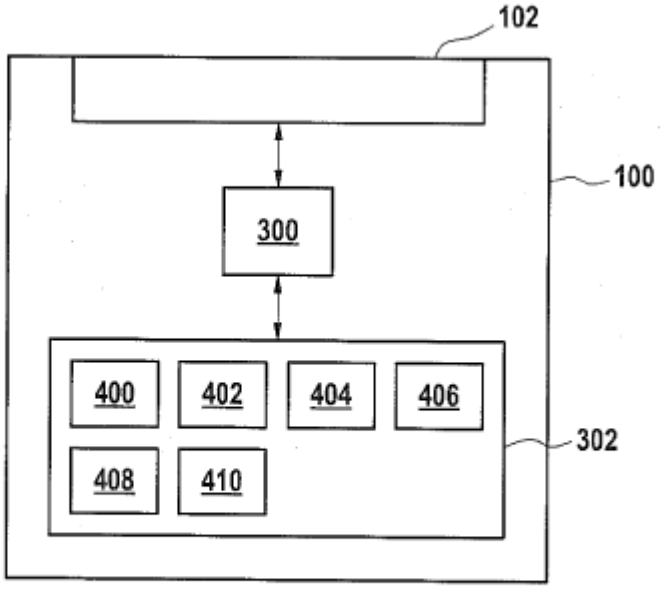


Fig. 5

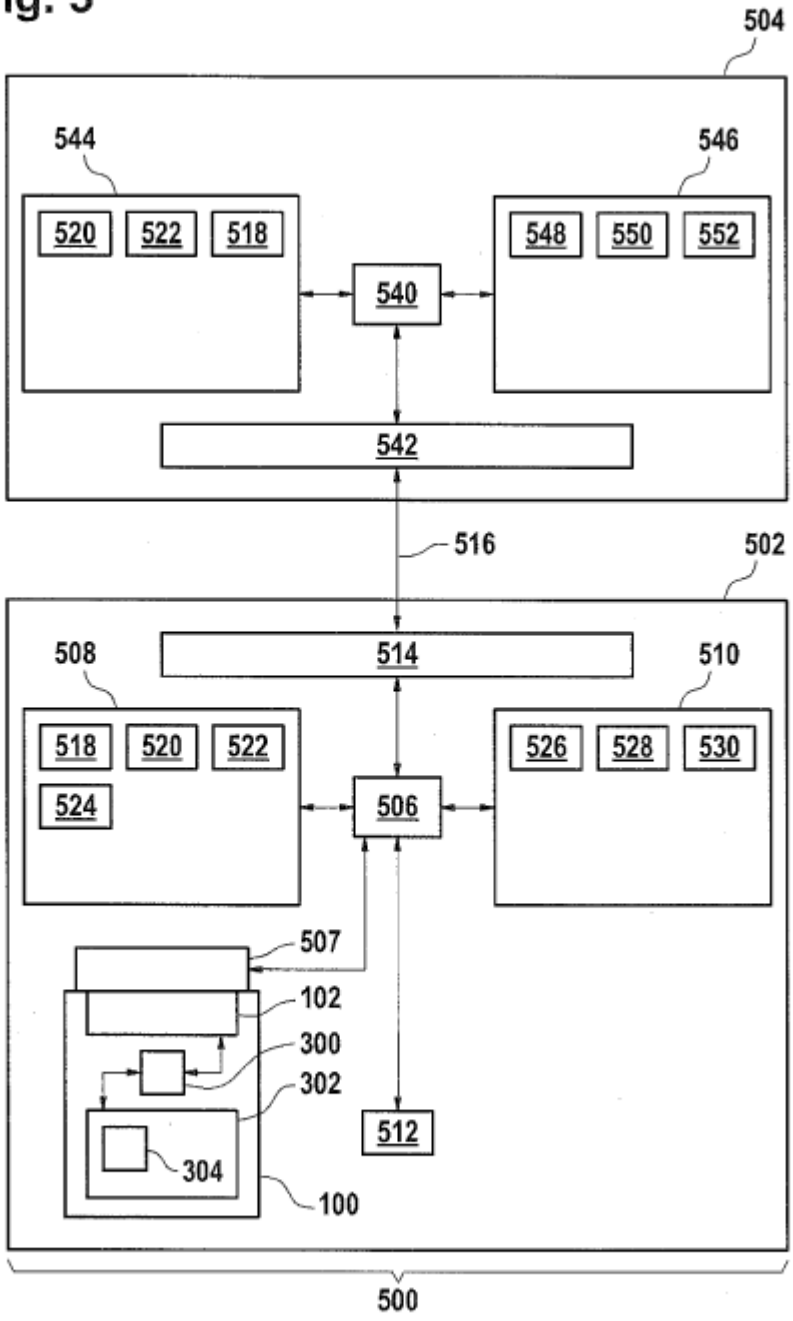

504
544
546
520
522
518
548
550
552
540
542
516
502
508
514
510
518
520
522
524
526
528
530
506
507
102
300
302
512
304
100
500

Fig. 6

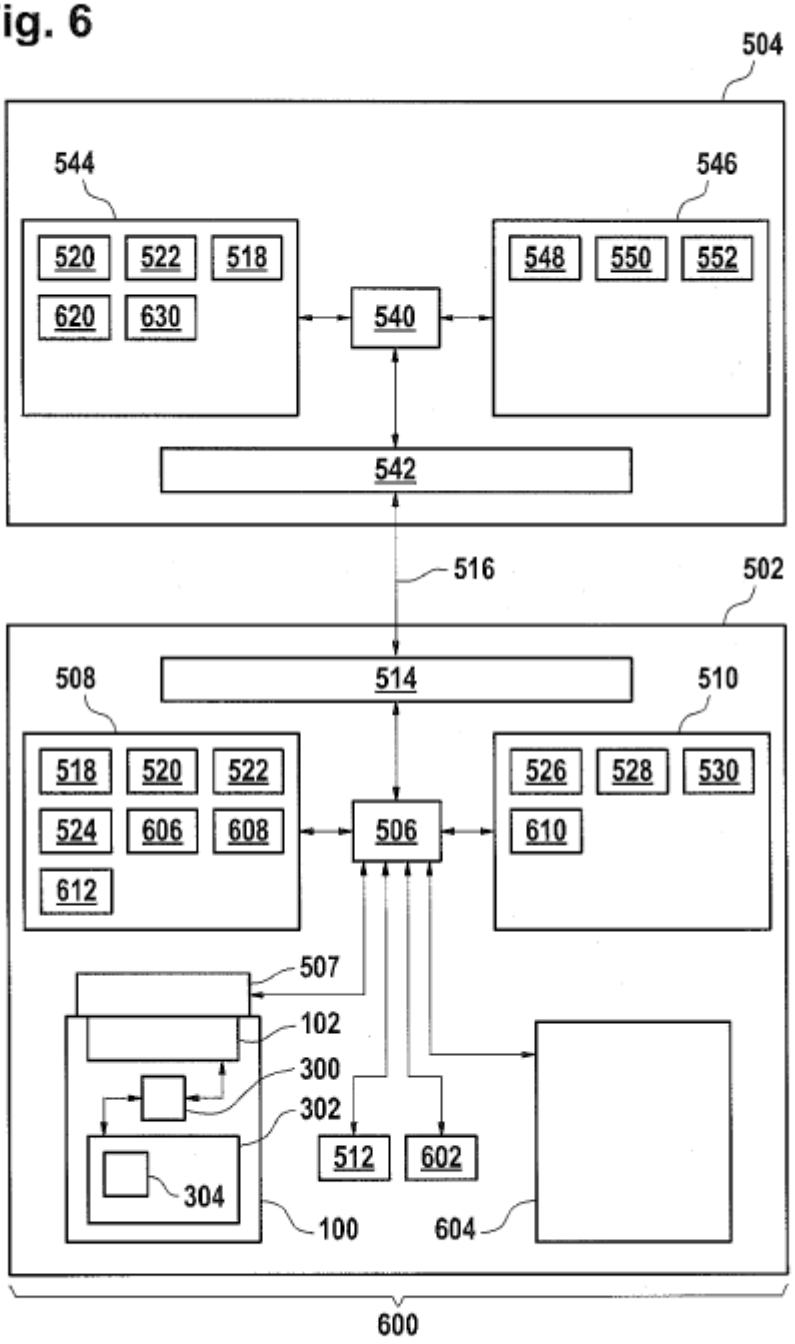
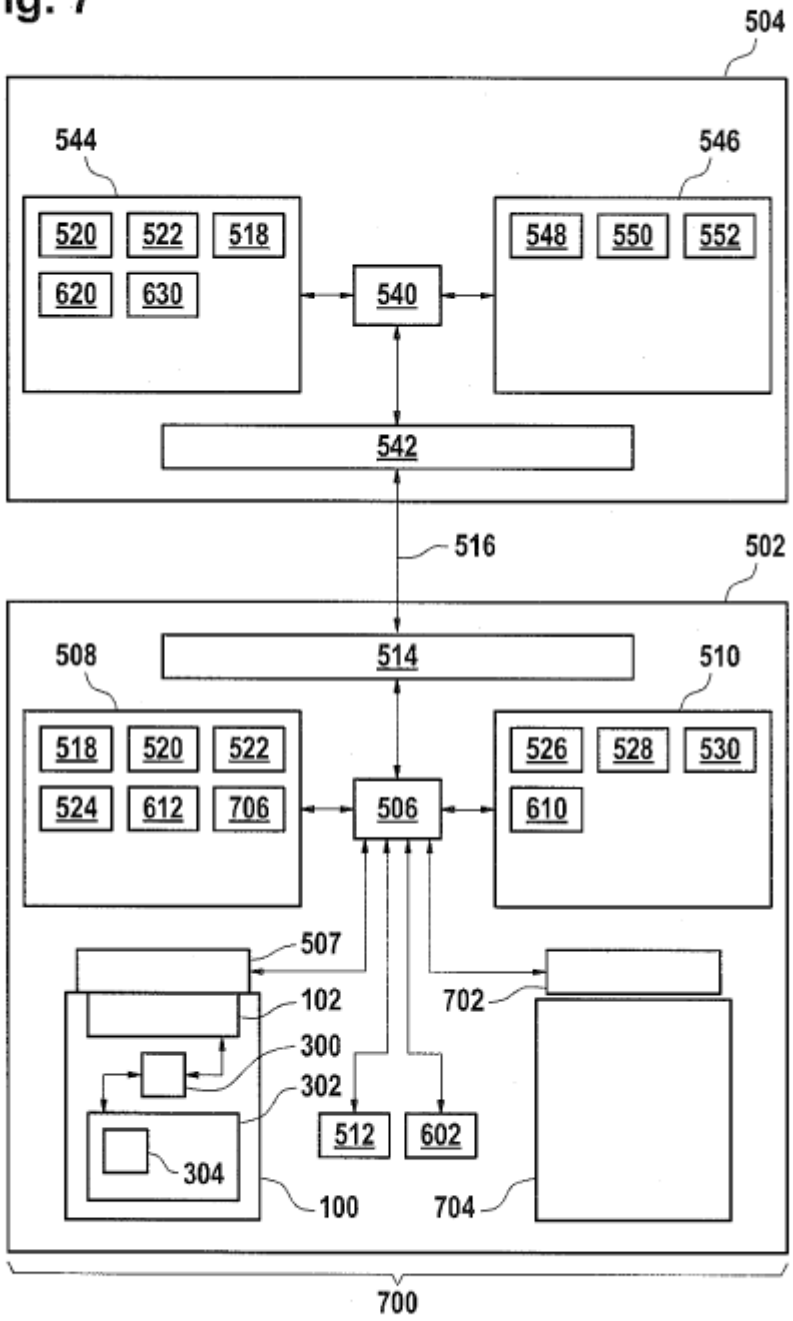

504
544
546
520
522
518
620
630
540
548
550
552
542
516
502
508
514
510
518
520
522
524
606
608
612
506
526
528
530
610
507
102
300
302
512
602
304
100
604
600

Fig. 7


504
544
546
520
522
518
620
630
540
548
550
552
542
516
502
508
514
510
518
520
522
524
612
706
506
526
528
530
610
507
102
702
300
302
512
602
304
100
704
700

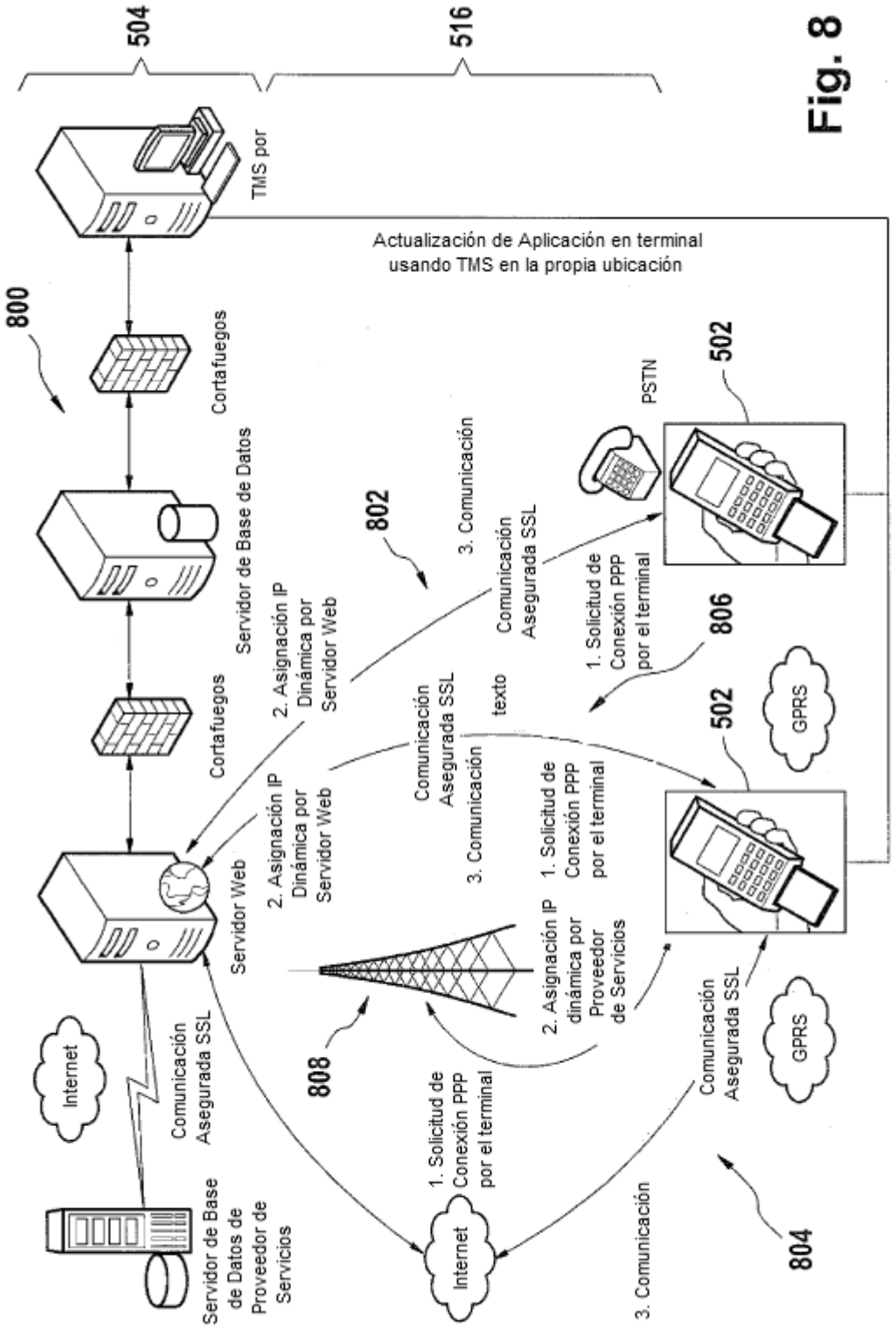

504
516
TMS por
Actualización de Aplicación en terminal
usando TMS en la propia ubicación
800
Cortafuegos
Servidor de Base de Datos
Cortafuegos
Servidor Web
802
3. Comunicación
Comunicación
Asegurada SSL
2. Asignación IP
Dinámica por
Servidor Web
1. Solicitud de
Conexión PPP
por el terminal
PSTN
502
806
texto
Comunicación
Asegurada SSL
3. Comunicación
1. Solicitud de
Conexión PPP
por el terminal
2. Asignación IP
Dinámica por
Servidor Web
GPRS
502
808
2. Asignación IP
dinámica por
Proveedor
de Servicios
Internet
Comunicación
Asegurada SSL
Internet
1. Solicitud de
Conexión PPP
por el terminal
GPRS
Comunicación
Asegurada SSL
Servidor de Base
de Datos de
Proveedor de
Servicios
3. Comunicación
804

Fig. 8

Fig. 9

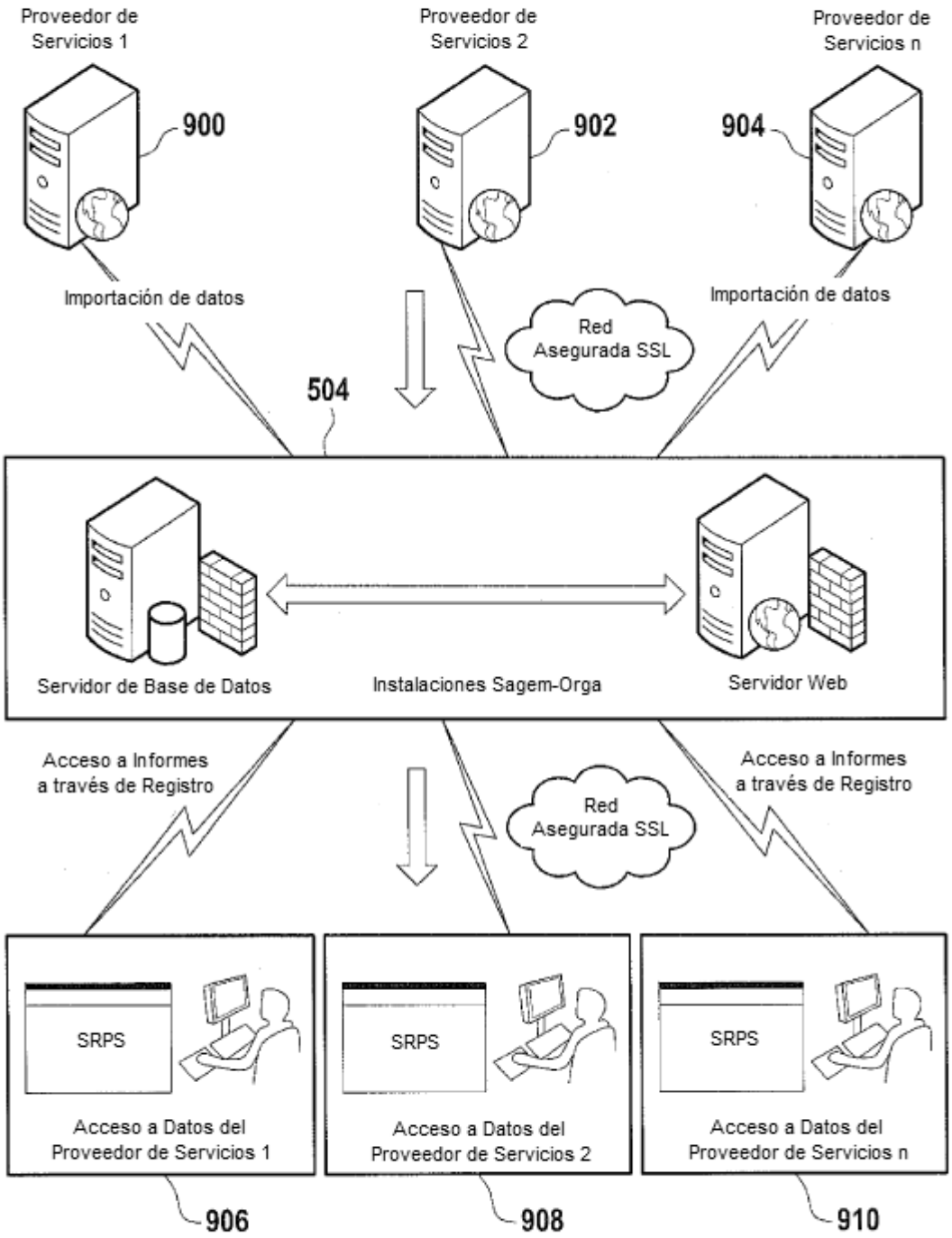

Proveedor de Servicios 1
Proveedor de Servicios 2
Proveedor de Servicios n
900
902
904
Importación de datos
Importación de datos
Red Asegurada SSL
504
Servidor de Base de Datos
Instalaciones Sagem-Orga
Servidor Web
Acceso a Informes a través de Registro
Red Asegurada SSL
Acceso a Informes a través de Registro
SRPS
SRPS
SRPS
Acceso a Datos del Proveedor de Servicios 1
Acceso a Datos del Proveedor de Servicios 2
Acceso a Datos del Proveedor de Servicios n
906
908
910

Fig. 10

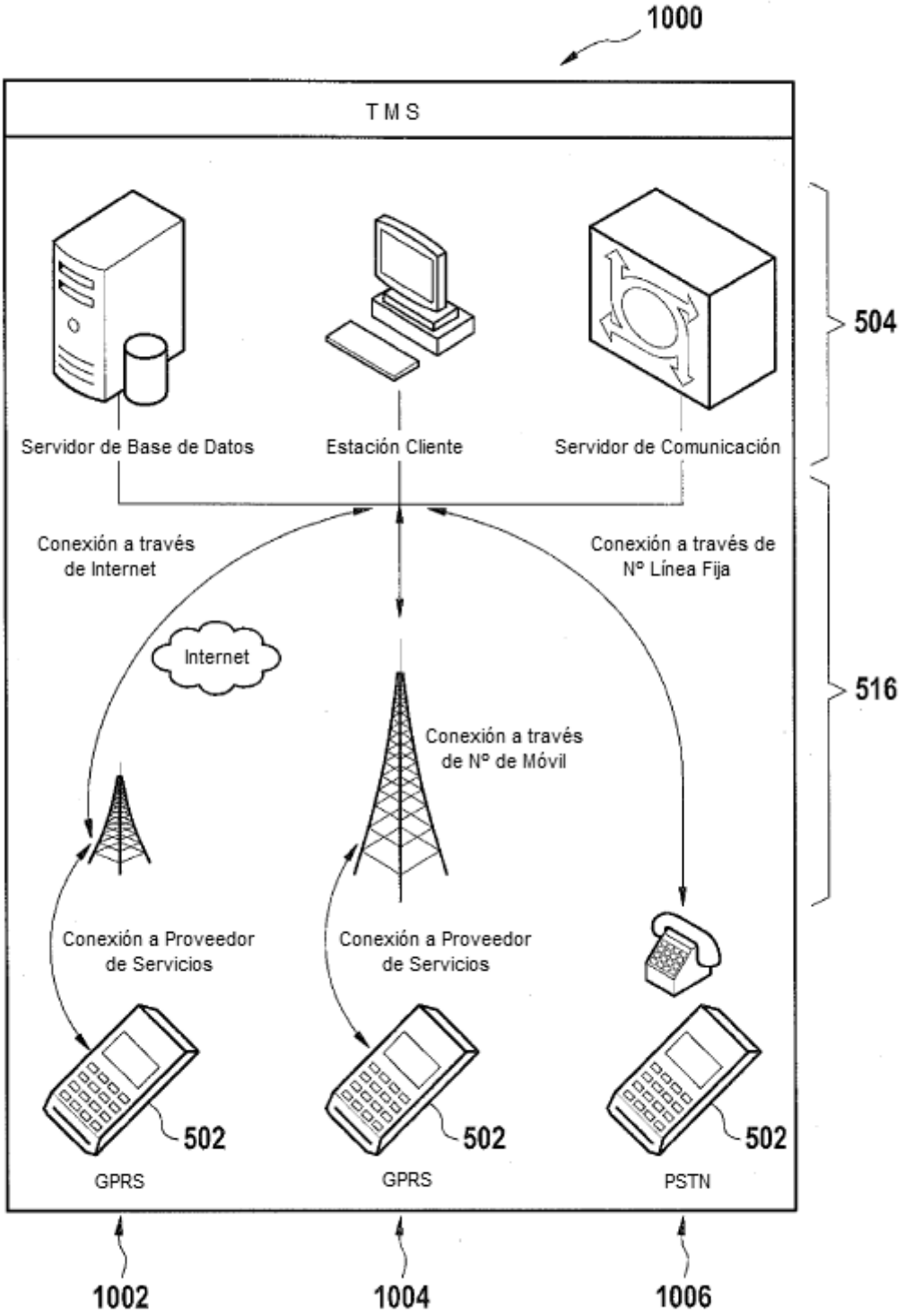

1000
TMS
Servidor de Base de Datos
Estación Cliente
Servidor de Comunicación
504
Conexión a través de Internet
Conexión a través de Nº Línea Fija
Internet
Conexión a través de Nº de Móvil
516
Conexión a Proveedor de Servicios
Conexión a Proveedor de Servicios
502
502
502
GPRS
GPRS
PSTN
1002
1004
1006

Fig. 11

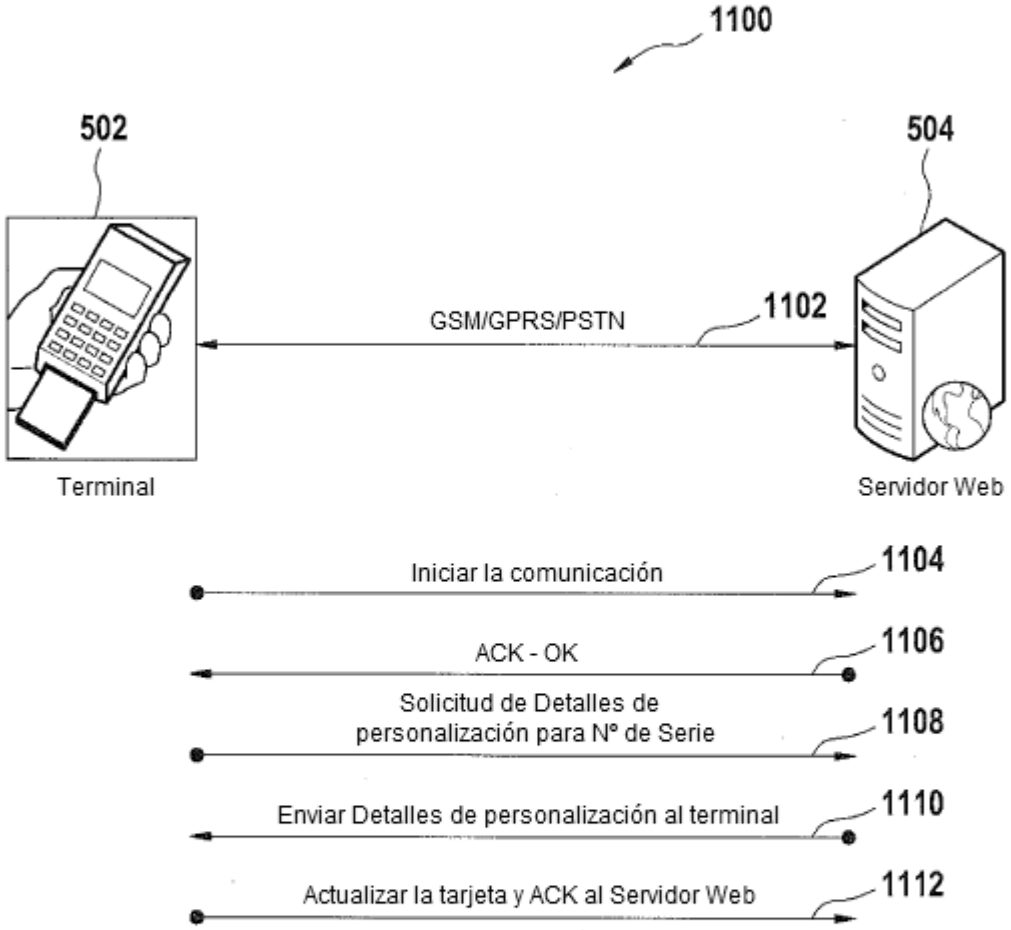

1100
502
504
GSM/GPRS/PSTN
1102
Terminal
Servidor Web
Iniciar la comunicación
1104
ACK - OK
1106
Solicitud de Detalles de personalización para N° de Serie
1108
Enviar Detalles de personalización al terminal
1110
Actualizar la tarjeta y ACK al Servidor Web
1112

Fig. 12

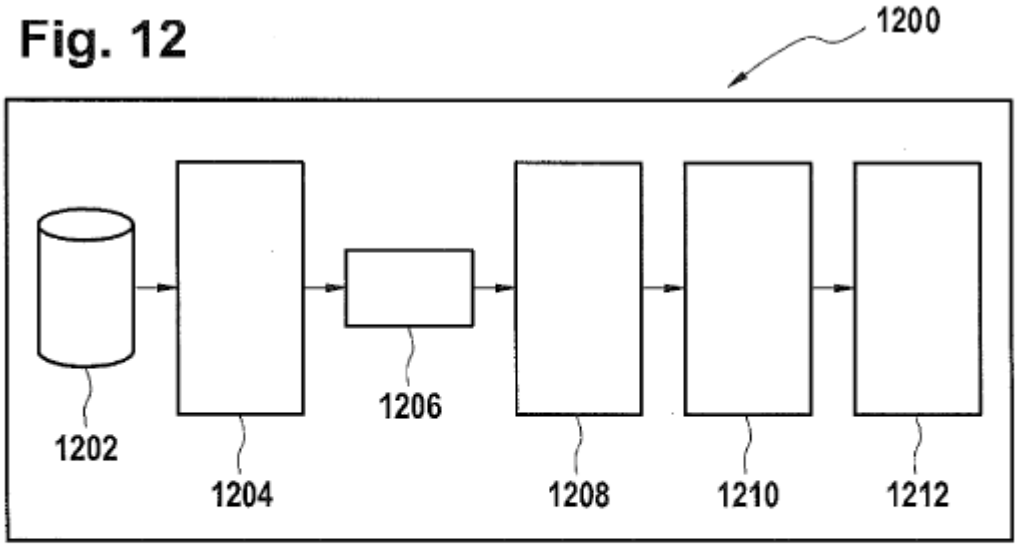


Fig. 13

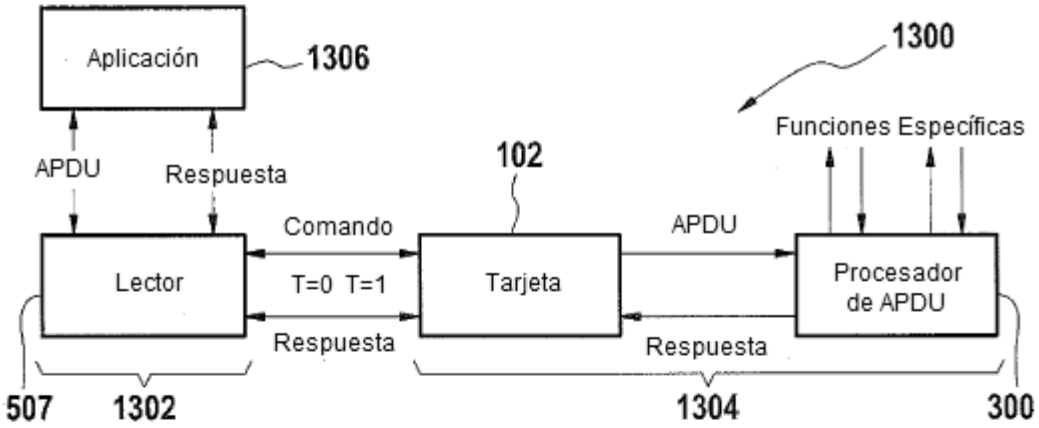


Fig. 14

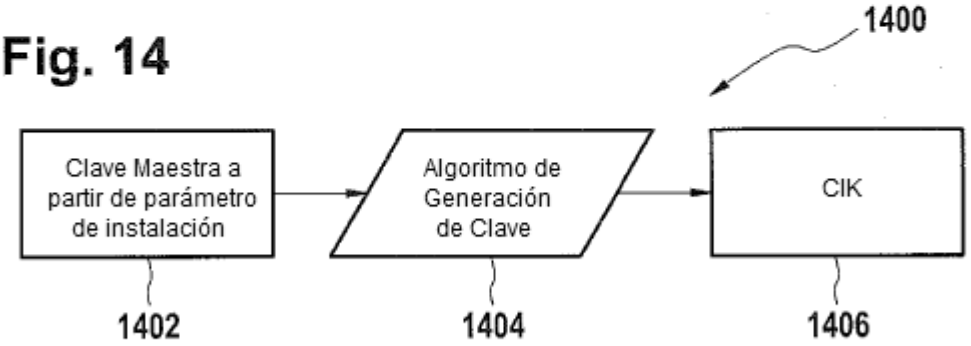
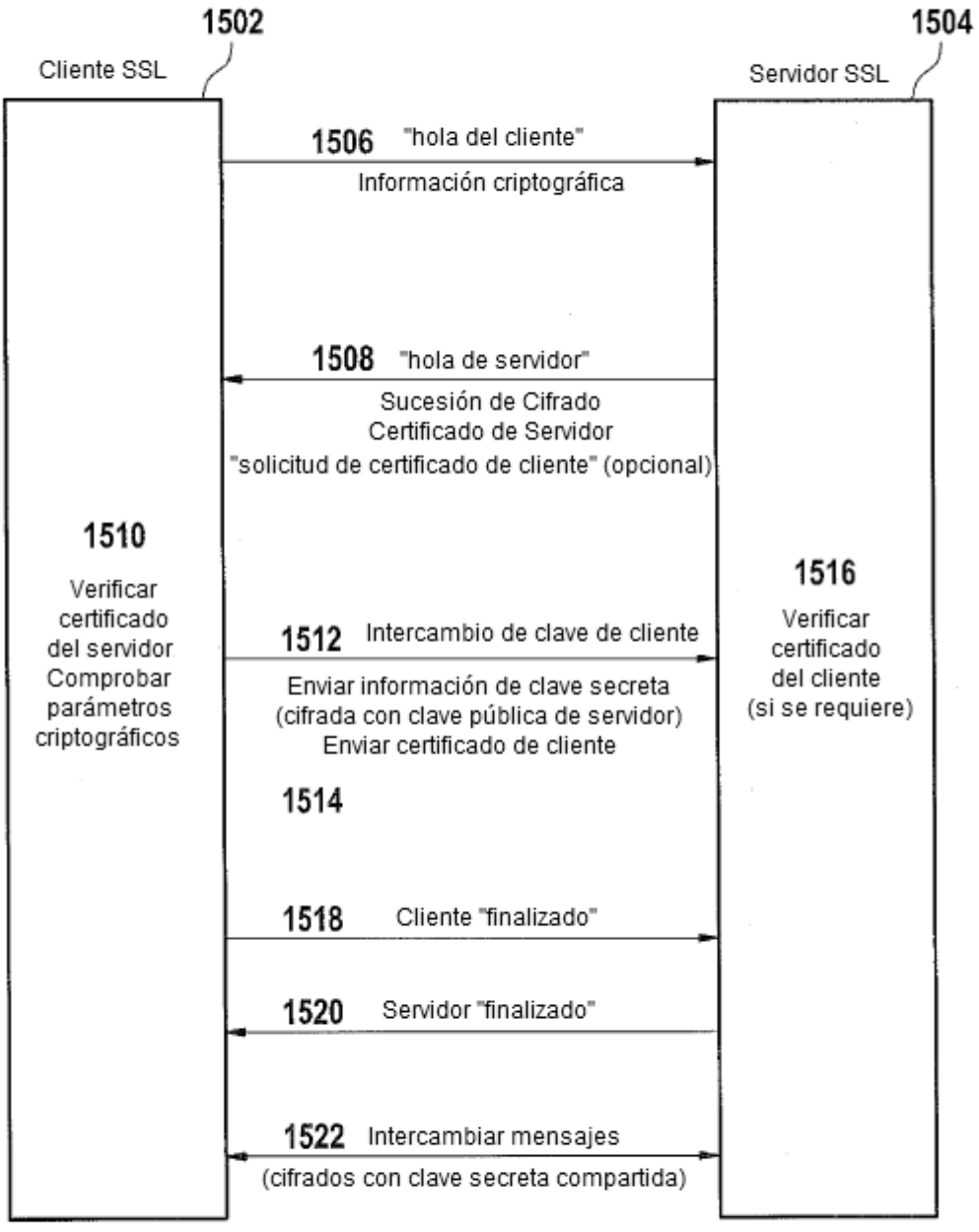


Fig. 15


1502
Cliente SSL
1504
Servidor SSL
1506 "hola del cliente"
Información criptográfica
1508 "hola de servidor"
Sucesión de Cifrado
Certificado de Servidor
"solicitud de certificado de cliente" (opcional)
1510
Verificar certificado del servidor
Comprobar parámetros criptográficos
1516
Verificar certificado del cliente (si se requiere)
1512 Intercambio de clave de cliente
Enviar información de clave secreta (cifrada con clave pública de servidor)
Enviar certificado de cliente
1514
1518 Cliente "finalizado"
1520 Servidor "finalizado"
1522 Intercambiar mensajes
(cifrados con clave secreta compartida)