(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 797 788**

(51) Int. CI.:

H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.09.2016 E 16188340 (0)**

(97) Fecha y número de publicación de la concesión europea: **25.03.2020 EP 3293912**

(54) Título: **Sistema de identificación de abonado**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.12.2020

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

KALINER, STEFAN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema de identificación de abonado

Ámbito técnico

La presente invención se refiere al ámbito de la tecnología de comunicaciones, en particular, a la identificación de un abonado en una red de comunicaciones.

Trasfondo técnico

Para determinadas aplicaciones, por ejemplo, en el contexto del Internet de las cosas móvil (mobile Internet-of-Things, mobile IoT), la utilización de tarjetas SIM (Subscriber Identity Module, SIM) clásicas está unida con desafíos, dado que las tarjetas SIM clásicas pueden presentar condiciones macro limitantes, por ejemplo, en relación a los costes, el tamaño constructivo y el consumo de energía.

La utilización de tarjetas SIM clásicas es además relativamente cara, debido a su fabricación exigente, altos requisitos de seguridad y el costo de manipulación físico en la logística en lo que se refiere a la funcionalidad básica proporcionada. Esto es válido entonces, en particular, cuando el precio total de un equipo de comunicaciones es muy bajo, como está previsto para equipos de comunicaciones futuros en el contexto del Internet de las cosas móvil. Los equipos de comunicaciones de este tipo comprenden, por ejemplo, sensores y actuadores interfaces de telefonía móvil así como módulos de transmisión de datos sencillos.

Además, los equipos de comunicaciones de este tipo no disponen habitualmente del espacio necesario para la integración de tarjetas SIM clásicas. Incluso formas constructivas no extraíbles de tarjetas SIM, por ejemplo, tarjetas SIM MFF (Machine-to-Machine Form Factor), exigen habitualmente todavía demasiado espacio para la integración en equipos de comunicaciones de este tipo. A esto hay que añadir, que hay que tener en cuenta el consumo de energía de tarjetas SIM clásicas, el cual en las presentes aplicaciones, las cuales por ejemplo prevén un funcionamiento con un único elemento de batería AAA durante un período de 5 años.

Las tarjetas SIM clásicas, en sus características disponibles actualmente parecen, por lo tanto, en el contexto del Internet de las cosas móvil, a causa de los altos requisitos en eficiencia de costes, tamaño constructivo y consumo de energía, ser utilizables solo de forma limitada.

El documento DE 10 2013 105 727 A1, da a conocer un procedimiento para la desactivación de un sistema de seguridad con utilización de un documento de identificación legible electrónicamente. En este caso, se puede leer una identificación electrónica del documento de identificación y compararla con una identificación electrónica previamente almacenada.

El documento DE 195 27 715 A1, da a conocer un procedimiento para la identificación de usuario y la autenticación de usuario en conexiones móviles de datos, en particular, para el sistema de telefonía móvil Modacom. En este caso, tiene lugar una autenticación de una tarjeta con chip con respecto a un equipo terminal con utilización de claves criptográficas.

El documento DE 10 2014 105 866 A1, da a conocer un procedimiento para prever un documento de identificación de una persona con un certificado criptográfico. En este caso, se transmiten una fecha de persona previamente almacenada y una clave criptográfica generada a un servidor de certificación electrónico. El certificado criptográfico se genera mediante el servidor de certificación electrónico y se transmite al documento de identificación.

El documento DE 10 2008 024 798 A1, da a conocer un procedimiento para la personalización por el aire (Over-The-Air) de tarjetas con chip en las telecomunicaciones. En este caso, un módulo de identificación de abonado se equipa antes de la primera puesta en funcionamiento con un conjunto no individual y provisional de parámetros de identificación y de autenticación iniciales, almacenándose después de una primera puesta en funcionamiento un conjunto de datos de abonado individual y definitivo en el módulo de identificación de abonado.

Descripción de la invención

Es por ello una misión de la presente invención, proporcionar un concepto eficiente para la identificación de un abonado en una red de comunicaciones.

Esta misión se resuelve mediante las características de las reivindicaciones independientes. Formas de realización ventajosas de la invención son objeto de la descripción, las figuras, así como de las reivindicaciones dependientes.

La presente invención se basa en el conocimiento de que la misión de arriba se puede resolver mediante un sistema de identificación de abonado optimizado para la implementación de la funcionalidad básica de una tarjeta SIM, pudiendo tener lugar una integración económica con el hardware restante de un equipo de comunicaciones, por ejemplo, en forma de un sistema en chip (SoC). Mediante una separación entre funciones no críticas en un primer módulo de circuito de conmutación y funciones críticas en un segundo módulo de circuito de conmutación, en el sentido de la seguridad de datos, se posibilita por lo tanto un diseño optimizado, en el que únicamente debería

implementarse de manera segura una porción muy reducida de funciones críticas. El primer módulo de circuito de conmutación puede, por consiguiente, presentar requisitos reducidos en cuanto a seguridad de datos que el segundo módulo de circuito de conmutación. De esta manera, se posibilita por ejemplo una integración sencilla del primer módulo de circuito de conmutación en un tercer módulo de circuito de conmutación del equipo de comunicaciones, pudiendo proporcionar el tercer módulo de circuito de conmutación la funcionalidad básica del equipo de comunicaciones. En caso de una integración completa de los tres módulos pueden tener importancia requisitos aumentados en cuanto a seguridad de datos, únicamente para la parte del segundo módulo de circuito de conmutación.

El número limitado de funciones críticas conduce, en este caso, a un potencial reducido para ataques a la seguridad de datos, un riesgo en general reducido para fallos y una comprobación y certificación más sencillas y, por lo tanto, más económicas. La posibilidad para la integración en forma de un sistema en chip (SoC) mínimo resuelve, en este caso, al mismo tiempo los desafíos previamente mencionados en el contexto del Internet de las cosas móvil, en particular, del consumo de energía, del tamaño constructivo y de la eficiencia de costes con alto número de unidades.

Por consiguiente, se puede realizar un sistema de identificación de abonado (Subscriber Identificaction System, SIS) altamente integrable, el cual posibilita una identificación del abonado. Además, puede tener lugar una autenticación del abonado.

De acuerdo con un primer aspecto, la invención se refiere a un sistema de identificación de abonado para la identificación de un abonado en una red de comunicaciones, estando asociados al abonado un identificador de identidad de abonado y una clave criptográfica. El sistema de identificación de abonado comprende un primer módulo de circuito de conmutación, en el cual está almacenado al menos el identificador de identidad de abonado, presentando el primer módulo de circuito de conmutación una primera interfaz de comunicaciones, la cual está configurada para recibir una señal de petición después del identificador de identidad de abonado y, en respuesta a la recepción de la señal de petición, enviar el identificador de identidad de abonado. El sistema de identificación de abonado comprende además un segundo módulo de circuito de conmutación, en el cual está almacenada al menos la clave criptográfica, presentando el segundo módulo de circuito de conmutación una segunda interfaz de comunicaciones, la cual está configurada para recibir un parámetro de entrada, estando el segundo módulo de circuito de conmutación configurado para vincular el parámetro de entrada con la clave criptográfica con utilización de un algoritmo para obtener un parámetro de salida y estando la segunda interfaz de comunicaciones configurada para enviar el parámetro de salida.

El abonado puede, por ejemplo, identificarse con utilización del identificador de identidad de abonado y autenticarse con utilización del parámetro de entrada y del parámetro de salida.

De acuerdo con una forma de realización, el primer módulo de circuito de conmutación comprende una primera memoria no volátil, estando almacenado al menos el identificador de identidad de abonado en la primera memoria no volátil, y el segundo módulo de circuito de conmutación comprende una segunda memoria no volátil, estando almacenada al menos la clave criptográfica en la segunda memoria no volátil. De esta manera, se logra la ventaja de que el identificador de identidad de abonado y la clave criptográfica pueden almacenarse de forma permanente.

La primera memoria no volátil y/o la segunda memoria no volátil pueden estar formadas, respectivamente, por una memoria de solo lectura programable borrable (Erasable Programmable Read-Only Memory, EPROM).

De acuerdo con una forma de realización, el segundo módulo de circuito de conmutación comprende un circuito lógico, estando el circuito lógico configurado para vincular el parámetro de entrada con la clave criptográfica con utilización del algoritmo. De esta manera, se logra la ventaja de que el parámetro de salida se puede determinar de manera eficiente en base al parámetro de entrada y al algoritmo.

El circuito lógico puede estar formado por un circuito lógico programable (Programmable Logic Device, PLD). El circuito lógico puede además estar enhebrado de conexiones fijas.

De acuerdo con una forma de realización, el segundo módulo de circuito de conmutación forma un módulo de seguridad hardware (en inglés, Hardware Security Module, HSM). De esta manera, se logra la ventaja de que el segundo módulo de circuito de conmutación puede utilizar funciones y propiedades de un módulo de seguridad hardware, las cuales dificultan un espionaje o una manipulación de la clave criptográfica y/o del algoritmo.

El segundo módulo de circuito de conmutación puede proteger la calve criptográfica y/o el algoritmo tanto contra ataques de tecnología software al igual que también físicos, así como contra ataques de canal lateral. El segundo módulo de circuito de conmutación puede estar configurado para detectar ataques o bien ataques de canal lateral y, en respuesta, a continuación borrar la clave criptográfica y/o el algoritmo. El segundo módulo de circuito de conmutación puede presentar además capas conductoras para el apantallamiento, para evitar una lectora no deseada de la clave criptográfica y/o del algoritmo en base a ondas electromagnéticas irradiadas. El segundo módulo de circuito de conmutación puede además estar configurado para detectar luz radiada en un rango de longitud de onda predeterminado o estados de funcionamiento no especificados del segundo módulo de circuito de conmutación y, en respuesta, a continuación borrar la clave criptográfica y/o el algoritmo. El segundo módulo de

circuito de conmutación utilizar además enfoques establecidos para el cifrado de bus. El segundo módulo de circuito de conmutación puede comprender además un procesador criptográfico seguro (en inglés, Secure Cryptoprocessor) o formar un procesador criptográfico seguro.

De acuerdo con una forma de realización, el sistema de identificación de abonado comprende un módulo de plataforma de confianza (TPM), comprendiendo el módulo de plataforma de confianza (TPM) el segundo módulo de circuito de conmutación. De esta manera, se logra la ventaja de que el segundo módulo de circuito de conmutación puede integrarse en el módulo de plataforma de confianza (TPM).

De acuerdo con una forma de realización, en el segundo módulo de circuito de conmutación está almacenado además el identificador de identidad de abonado. De esta manera, se logra la ventaja de que se puede garantizar de forma eficiente una asociación del identificador de identidad de abonado a la clave criptográfica.

De acuerdo con una forma de realización, el identificador de identidad de abonado es una Identidad Internacional del Abonado Móvil (IMSI). De esta manera, se logra la ventaja de que se puede utilizar una forma estandarizada de un identificador de identidad de abonado.

De acuerdo con una forma de realización, el algoritmo es un algoritmo A3/A8, un algoritmo MILENAGE o un algoritmo TUAK. De esta manera, se logra la ventaja de que se pueden utilizar algoritmos de autenticación estandarizados.

La componente A3 del algoritmo A3/A8 puede servir para la autenticación. La componente A8 del algoritmo A3/A8 puede servir para el cifrado de la comunicación. Las dos componentes pueden estar realizadas juntas, pudiendo proporcionarse en cada autenticación una clave nueva para el cifrado de la comunicación. El parámetro de salida se puede utilizar para los dos fines. El algoritmo MILENAGE y el algoritmo TUAK también pueden utilizarse para la autenticación y la generación de claves. El algoritmo A3/A8, el algoritmo MILENAGE y el algoritmo TUAK pueden implementarse de acuerdo con el correspondiente estándar ETSI o bien estándar 3GPP.

De acuerdo con una forma de realización, la clave criptográfica puede estar almacenada de manera no legible en el segundo módulo de circuito de conmutación. De esta manera, se logra la ventaja de que la clave criptográfica está vinculada criptográficamente al segundo módulo de circuito de conmutación.

De acuerdo con un segundo aspecto, la invención se refiere a un equipo de comunicaciones para la comunicación con un servidor de autenticación a través de una red de comunicaciones. El equipo de comunicaciones comprende un sistema de identificación de abonado de acuerdo con el primer aspecto de la invención. El equipo de comunicaciones comprende además un tercer módulo de circuito de conmutación con una tercera interfaz de comunicaciones para la comunicación con el sistema de identificación de abonado y una cuarta interfaz de comunicaciones para la comunicación con el servidor de autenticación a través de la red de comunicaciones. La tercera interfaz de comunicaciones está configurada para enviar la señal de petición al sistema de identificación de abonado y recibir el identificador de identidad de abonado desde el sistema de identificación de abonado. La cuarta interfaz de comunicaciones está configurada para enviar el identificador de identidad de abonado al servidor de autenticación a través de la red de comunicaciones.

El tercer módulo de circuito de conmutación puede comprender además un procesador e interfaces adicionales del equipo de comunicaciones, por ejemplo, para la interacción con el abonado.

El servidor de autenticación puede ser parte de un centro de autenticación (Authentication Center, AuC) de la red de comunicaciones.

De acuerdo con una forma de realización, la cuarta interfaz de comunicaciones está además configurada para recibir el parámetro de entrada desde el servidor de autenticación a través de la red de comunicaciones, estando la tercera interfaz de comunicaciones además configurada para enviar el parámetro de entrada al sistema de identificación de abonado y recibir el parámetro de salida desde el sistema de identificación de abonado, y estando la cuarta interfaz de comunicaciones además configurada para enviar el parámetro de salida al servidor de autenticación a través de la red de comunicaciones. De esta manera, se logra la ventaja de que puede tener lugar una autenticación eficiente del abonado.

De acuerdo con una forma de realización, el tercer módulo de circuito de conmutación comprende el primer módulo de circuito de conmutación del sistema de identificación de abonado y/o el segundo módulo de circuito de conmutación del sistema de identificación de abonado. De esta manera, se logra la ventaja de que se puede lograr una implementación eficiente.

De acuerdo con una forma de realización, el primer módulo de circuito de conmutación está dispuesto en un primer circuito integrado. De esta manera, se logra la ventaja de que el primer módulo de circuito de conmutación se puede implementar de manera eficiente.

De acuerdo con una forma de realización, el segundo módulo de circuito de conmutación está dispuesto en un segundo circuito integrado. De esta manera, se logra la ventaja de que el segundo módulo de circuito de conmutación se puede implementar de manera eficiente.

De acuerdo con una forma de realización, el tercer módulo de circuito de conmutación está dispuesto en un tercer circuito integrado. De esta manera, se logra la ventaja de que el tercer módulo de circuito de conmutación se puede implementar de manera eficiente.

De acuerdo con una forma de realización, el primer módulo de circuito de conmutación está dispuesto en un primer circuito integrado, estando el segundo módulo de circuito de conmutación dispuesto en un segundo circuito integrado y estando el tercer módulo de circuito de conmutación dispuesto en un tercer circuito integrado. De esta manera, se logra la ventaja de que los módulos de circuito de conmutación se pueden implementar individuales, respectivamente, de manera eficiente.

De acuerdo con una forma de realización, el primer módulo de circuito de conmutación, el segundo módulo de circuito de conmutación y el tercer módulo de circuito de conmutación están dispuestos en un circuito integrado común. De esta manera, se logra la ventaja de que los módulos de circuito de conmutación se pueden implementar conjuntamente de manera eficiente.

De acuerdo con un tercer aspecto, la invención se refiere a un procedimiento para la identificación de un abonado en una red de comunicaciones con utilización de un sistema de identificación de abonado. Al abonado están asociados un identificador de identidad de abonado y una clave criptográfica. El sistema de identificación de abonado comprende un primer módulo de circuito de conmutación con una primera interfaz de comunicaciones y un segundo módulo de circuito de conmutación con una segunda interfaz de comunicaciones, estando en el primer módulo de circuito de conmutación almacenado al menos el identificador de identidad de abonado y estando en el segundo módulo de circuito de conmutación almacenada al menos la clave criptográfica. El procedimiento comprende una recepción de una señal de petición después del identificador de identidad de abonado mediante una primera interfaz de comunicaciones, en respuesta a la recepción de la señal de petición, un envío del identificador de identidad de abonado mediante la primera interfaz de comunicaciones, una recepción de un parámetro de entrada mediante la segunda interfaz de comunicaciones, una vinculación del parámetro de entrada con la clave criptográfica con utilización de un algoritmo mediante el segundo módulo de circuito de conmutación, para obtener un parámetro de salida, y un envío del parámetro de salida mediante la segunda interfaz de comunicaciones.

El procedimiento puede realizarse mediante el sistema de identificación de abonado. Otras características del procedimiento resultan directamente a partir de las características o la funcionalidad del sistema de identificación de abonado.

De acuerdo con un cuarto aspecto, la invención se refiere a un procedimiento para la comunicación con un servidor de autenticación a través de una red de comunicaciones con utilización de un equipo de comunicaciones. El equipo de comunicaciones comprende un sistema de identificación de abonado de acuerdo con el primer aspecto de la invención y un tercer módulo de circuito de conmutación con una tercera interfaz de comunicaciones para la comunicación con el sistema de identificación de abonado y una cuarta interfaz de comunicaciones para la comunicación con el servidor de autenticación a través de la red de comunicaciones. El procedimiento comprende un envío de la señal de petición al sistema de identificación de abonado mediante la tercera interfaz de comunicaciones, una recepción del identificador de identidad de abonado por el sistema de identificación de abonado mediante la tercera interfaz de comunicaciones y un envío del identificador de identidad de abonado recibido al servidor de autenticación a través de la red de comunicaciones mediante la cuarta interfaz de comunicaciones.

El procedimiento puede realizarse mediante el equipo de comunicaciones. Otras características del procedimiento resultan directamente a partir de las características o la funcionalidad del equipo de comunicaciones.

De acuerdo con un quinto aspecto, la invención se refiere a un programa informático con un código de programa para la ejecución del procedimiento de acuerdo con el tercer aspecto de la invención o del procedimiento de acuerdo con el cuarto aspecto de la invención.

El sistema de identificación de abonado y/o el equipo de comunicaciones pueden estar configurados mediante programación para ejecutar el código de programa.

La invención puede realizarse en hardware y/o en software.

Descripción de las figuras

Otros ejemplos de realización se explican más en detalle con referencia a las figuras adjuntas. Muestran:

la Fig. 1, un diagrama esquemático de un sistema de identificación de abonado para la identificación de un abonado en una red de comunicaciones;

la Fig. 2, un diagrama esquemático de un equipo de comunicaciones para la comunicación con un servidor de autenticación a través de una red de comunicaciones;

la Fig. 3, un diagrama esquemático de un equipo de comunicaciones para la comunicación con un servidor de autenticación a través de una red de comunicaciones;

la Fig. 4, un diagrama esquemático de un equipo de comunicaciones para la comunicación con un servidor de autenticación a través de una red de comunicaciones;

la Fig. 5, un diagrama esquemático de un equipo de comunicaciones para la comunicación con un servidor de autenticación a través de una red de comunicaciones;

la Fig. 6, un diagrama esquemático de un equipo de comunicaciones para la comunicación con un servidor de autenticación a través de una red de comunicaciones;

la Fig. 7, un diagrama esquemático de un equipo de comunicaciones para la comunicación con un servidor de autenticación a través de una red de comunicaciones;

la Fig. 8, un diagrama esquemático de un equipo de comunicaciones para la comunicación con un servidor de autenticación a través de una red de comunicaciones;

la Fig. 9, un diagrama esquemático de un procedimiento para la identificación de un abonado en una red de comunicaciones con utilización de un sistema de identificación de abonado; y

la Fig. 10, un diagrama esquemático de un procedimiento para la comunicación con un servidor de autenticación a través de una red de comunicaciones con utilización de un equipo de comunicaciones.

Descripción detallada de las figuras

La Fig. 1 muestra un diagrama esquemático de un sistema 100 de identificación de abonado para la identificación de un abonado en una red de comunicaciones. Al abonado están asociados un identificador de identidad de abonado y una clave K criptográfica.

El sistema 100 de identificación de abonado comprende un primer módulo 101 de circuito de conmutación, en el cual está almacenado al menos el identificador de identidad de abonado, presentando el primer módulo 101 de circuito de conmutación una primera interfaz 103 de comunicaciones, la cual está configurada para recibir una señal de petición después del identificador de identidad de señal y, en respuesta a la recepción de la señal de petición, enviar el identificador de identidad de abonado. El sistema 100 de identificación de abonado comprende además un segundo módulo 105 de circuito de conmutación, en el cual está almacenada al menos la clave K criptográfica, presentado el segundo módulo 105 de circuito de conmutación una segunda interfaz 107 de comunicaciones, la cual está configurada para recibir un parámetro I de entrada, estando el segundo módulo 105 de circuito de conmutación configurado para vincular el parámetro I de entrada con la clave K criptográfica con utilización de un algoritmo A para obtener un parámetro O de salida y estando la segunda interfaz 107 de comunicaciones configurada para enviar el parámetro O de salida.

La Fig. 2 muestra un diagrama esquemático de un equipo 200 de comunicaciones para la comunicación con un servidor 207 de autenticación a través de una red 209 de comunicaciones. El equipo de comunicaciones comprende un sistema 100 de identificación de abonado y un tercer módulo 201 de circuito de conmutación.

El sistema 100 de identificación de abonado sirve para la identificación de un abonado en la red 209 de comunicaciones. Al abonado están asociados un identificador de identidad de abonado y una clave K criptográfica.

El sistema 100 de identificación de abonado comprende un primer módulo 101 de circuito de conmutación, en el cual está almacenado al menos el identificador de identidad de abonado, presentando el primer módulo 101 de circuito de conmutación una primera interfaz 103 de comunicaciones, la cual está configurada para recibir una señal de petición después del identificador de identidad de abonado y, en respuesta a la recepción de la señal de petición, enviar el identificador de identidad de abonado. El sistema 100 de identificación de abonado comprende además un segundo módulo 105 de circuito de conmutación, en el cual está almacenada al menos la clave K criptográfica, presentado el segundo módulo 105 de circuito de conmutación una segunda interfaz 107 de comunicaciones, la cual está configurada para recibir un parámetro I de entrada, estando el segundo módulo 105 de circuito de conmutación configurado para vincular el parámetro I de entrada con la clave K criptográfica con utilización de un algoritmo A para obtener un parámetro O de salida y estando la segunda interfaz 107 de comunicaciones configurada para enviar el parámetro O de salida.

El tercer módulo 201 de circuito de conmutación comprende una tercera interfaz 203 de comunicaciones para la comunicación con el sistema 100 de identificación de abonado y una cuarta interfaz 205 de comunicaciones para la comunicación con el servidor 207 de autenticación a través de la red 209 de comunicaciones. La tercera interfaz 203 de comunicaciones está configurada para enviar la señal de petición al sistema 100 de identificación de abonado y recibir el identificador de identidad de abonado desde el sistema 100 de identificación de abonado. La cuarta interfaz

205 de comunicaciones está configurada para enviar el identificador de identidad de abonado recibido al servidor 207 de autenticación a través de la red 209 de comunicaciones. Por consiguiente, el abonado puede identificarse mediante el servidor 207 de autenticación.

La cuarta interfaz 205 de comunicaciones está además configurada para recibir el parámetro I de entrada desde el servidor 207 de autenticación a través de la red 209 de comunicaciones, estando la tercera interfaz 203 de comunicaciones además configurada para enviar el parámetro I de entrada al sistema 100 de identificación de abonado y recibir el parámetro O de salida desde el sistema 100 de identificación de abonado, y estando la cuarta interfaz 205 de comunicaciones además configurada para enviar el parámetro O de salida al servidor 207 de autenticación a través de la red 209 de comunicaciones. Por consiguiente, el abonado puede autenticarse mediante el servidor 207 de autenticación, por ejemplo, en base a un enfoque de desafío-respuesta.

La Fig. 3 muestra un diagrama esquemático de un equipo 200 de comunicaciones para la comunicación con un servidor de autenticación a través de una red de comunicaciones. El equipo 200 de comunicaciones mostrado es una forma de realización posible del equipo 200 de comunicaciones de la Fig. 2.

El equipo 200 de comunicaciones comprende un sistema 100 de identificación de abonado con un primer módulo 101 de circuito de conmutación y un segundo módulo 105 de circuito de conmutación, así como un tercer módulo 201 de circuito de conmutación. El primer módulo 101 de circuito de conmutación puede realizarse como módulo no seguro, el segundo módulo 105 de circuito de conmutación puede realizarse como módulo seguro y el tercer módulo 201 de circuito de conmutación puede realizar una funcionalidad de orden superior del equipo 200 de comunicaciones. El identificador de identidad de abonado es una Identidad Internacional del Abonado Móvil (IMSI).

Por consiguiente, se puede utilizar un sistema 100 de identificación de abonado (en inglés, Subscriber Identity System, SIS) de dos piezas, con un primer módulo 101 de circuito de conmutación con solo una memoria no volátil y un segundo módulo 105 de circuito de conmutación con una memoria no volátil y un circuito lógico programable.

En este caso, el segundo módulo 105 de circuito de conmutación obtiene, en el caso más sencillo, solo una clave K criptográfica como clave de autenticación y un algoritmo A. La ejecución del algoritmo A puede iniciarse desde fuera mediante entrega de un parámetro I de entrada, con lo cual, con ayuda de la clave K criptográfica secreta, se genera un parámetro O de salida, es decir, O = A(I, K). El parámetro O de salida se devuelve en este caso, sin que la clave K criptográfica o el algoritmo A sean visibles hacia fuera. El segundo módulo 105 de circuito de conmutación sirve, por consiguiente, por si solo para la ejecución del algoritmo A. Contiene además una funcionalidad adicional para el almacenamiento de la clave K criptográfica.

El primer módulo 101 de circuito de conmutación comprende otros datos opcionales relevantes, en el caso más sencillo, sin embargo, solo el identificador de identidad de abonado o bien IMSI del abonado. Los datos del primer módulo 101 de circuito de conmutación habitualmente no son críticos y pueden almacenarse y leerse desde fuera.

El sistema 100 de identificación de abonado se asocia o bien personaliza a una relación de abonado, al almacenarse una combinación de identificador de identidad de abonado y clave K criptográfica. La clave K criptográfica se almacena, en este caso, en el segundo módulo 105 de circuito de conmutación y el identificador de identidad de abonado en el primer módulo 101 de circuito de conmutación.

Para el funcionamiento del equipo 200 de comunicaciones, el tercer módulo 201 de circuito de conmutación puede acceder a los módulos 101, 105 de circuito de conmutación como funcionalidad de orden superior y, por ejemplo, leer el identificador de identidad de abonado del primer módulo 101 de circuito de conmutación y realizar una autenticación con respecto a la red 209 de comunicaciones, por ejemplo, una red de telefonía móvil, con utilización del segundo módulo 105 de circuito de conmutación. En resumen, de esto resulta una funcionalidad básica de una tarjeta SIM clásica, la cual desde el punto de vista de la red 209 de comunicaciones no se diferencia de ésta. El equipo 200 de comunicaciones puede ser, por ejemplo, un equipo terminal en el contexto del Internet de las cosas.

De acuerdo con una forma de realización, el primer módulo 101 de circuito de conmutación se integra de forma lógica en el tercer módulo 201 de circuito de conmutación como funcionalidad de orden superior del equipo 200 de comunicaciones, por ejemplo, en una memoria del aparato 200 de comunicaciones, y el segundo módulo 105 de circuito de conmutación se implementa en un procesador, por ejemplo, el procesador principal, del equipo 200 de comunicaciones como sistema en chip (SoC). En esta forma se pueden realizar las ventajas nombradas arriba de manera particularmente ventajosa. El equipo 200 de comunicaciones puede, por consiguiente, realizarse como sistema en chip con un circuito integrado común para los módulos 101, 105, 201 de circuito de conmutación.

La Fig. 4 muestra un diagrama esquemático de un equipo 200 de comunicaciones para la comunicación con un servidor de autenticación a través de una red de comunicaciones. El equipo 200 de comunicaciones mostrado es una forma de realización posible del equipo 200 de comunicaciones de la Fig. 2.

El equipo 200 de comunicaciones comprende un sistema de identificación de abonado con un primer módulo 101 de circuito de conmutación y un segundo módulo 105 de circuito de conmutación, así como un tercer módulo 201 de circuito de conmutación. El primer módulo 101 de circuito de conmutación puede realizarse como módulo no seguro, el segundo módulo 105 de circuito de conmutación puede realizarse como módulo seguro y el tercer módulo 201 de

circuito de conmutación puede realizar una funcionalidad de orden superior del equipo 200 de comunicaciones. El identificador de identidad de abonado es una Identidad Internacional del Abonado Móvil (IMSI).

El primer módulo 101 de circuito de conmutación y el segundo módulo 105 de circuito de conmutación están dispuestos en el mismo circuito (chip) integrado. El primer módulo 101 de circuito de conmutación está integrado en el tercer módulo 201 de circuito de conmutación como funcionalidad de orden superior.

El primer módulo 101 de circuito de conmutación está, por consiguiente, integrado en el tercer módulo 201 de circuito de conmutación como funcionalidad de orden superior e incluido con el segundo módulo 105 de circuito de conmutación como sistema en chip en un circuito integrado común. Esta configuración puede ser particularmente ventajosa en el sentido de una solución ahorradora de costes, de espacio y de energía.

La Fig. 5 muestra un diagrama esquemático de un equipo 200 de comunicaciones para la comunicación con un servidor de autenticación a través de una red de comunicaciones. El equipo 200 de comunicaciones es una forma de realización posible del equipo 200 de comunicaciones de la Fig. 2.

El equipo 200 de comunicaciones comprende un sistema de identificación de abonado con un primer módulo 101 de circuito de conmutación y un segundo módulo 105 de circuito de conmutación, así como un tercer módulo 201 de circuito de conmutación. El primer módulo 101 de circuito de conmutación puede realizarse como módulo no seguro, el segundo módulo 105 de circuito de conmutación puede realizarse como módulo seguro y el tercer módulo 201 de circuito de conmutación puede realizar una funcionalidad de orden superior del equipo 200 de comunicaciones. El identificador de identidad de abonado es una Identidad Internacional del Abonado Móvil (IMSI).

El segundo módulo 105 de circuito de conmutación está dispuesto en un circuito (chip) integrado separado. El primer módulo 101 de circuito de conmutación está integrado en el tercer módulo 201 de circuito de conmutación como funcionalidad de orden superior.

El primer módulo 101 de circuito de conmutación está, por consiguiente, integrado en el tercer módulo 201 de circuito de conmutación como funcionalidad de orden superior y el segundo módulo 105 de circuito de conmutación está configurado como circuito (chip) integrado separado. La clave K criptográfica puede, por consiguiente, cargarse en un entorno seguro y el segundo módulo 105 de circuito de conmutación añadirse a continuación en un entorno no seguro en el equipo 200 de comunicaciones.

La Fig. 6 muestra un diagrama esquemático de un equipo 200 de comunicaciones para la comunicación con un servidor de autenticación a través de una red de comunicaciones. El equipo 200 de comunicaciones de comunicaciones mostrado es una forma de realización posible del equipo 200 de comunicaciones de la Fig. 2.

El equipo 200 de comunicaciones comprende un sistema de identificación de abonado con un primer módulo 101 de circuito de conmutación y un segundo módulo 105 de circuito de conmutación, así como un tercer módulo 201 de circuito de conmutación. El primer módulo 101 de circuito de conmutación puede realizarse como módulo no seguro, el segundo módulo 105 de circuito de conmutación puede realizarse como módulo seguro y el tercer módulo 201 de circuito de conmutación puede realizar una funcionalidad de orden superior del equipo 200 de comunicaciones. El identificador de identidad de abonado es una Identidad Internacional del Abonado Móvil (IMSI).

El primer módulo 101 de circuito de conmutación y el segundo módulo 105 de circuito de conmutación están dispuestos en circuitos (chips) integrados separados. En este caso, no tiene lugar una integración con el tercer módulo 201 de circuito de conmutación como funcionalidad de orden superior.

Por consiguiente, el primer módulo 101 de circuito de conmutación y el segundo módulo 105 de circuito de conmutación están configurados como circuitos (chips) integrados separados, o bien, están integrados en circuitos (chips) integrados separados.

La Fig. 7 muestra un diagrama esquemático de un equipo 200 de comunicaciones para la comunicación con un servidor de autenticación a través de una red de comunicaciones. El equipo 200 de comunicaciones de comunicaciones mostrado es una forma de realización posible del equipo 200 de comunicaciones de la Fig. 2.

El equipo 200 de comunicaciones comprende un sistema de identificación de abonado con un primer módulo 101 de circuito de conmutación y un segundo módulo 105 de circuito de conmutación, así como un tercer módulo 201 de circuito de conmutación. El primer módulo 101 de circuito de conmutación puede realizarse como módulo no seguro, el segundo módulo 105 de circuito de conmutación puede realizarse como módulo seguro y el tercer módulo 201 de circuito de conmutación puede realizar una funcionalidad de orden superior del equipo 200 de comunicaciones. El identificador de identidad de abonado es una Identidad Internacional del Abonado Móvil (IMSI).

El primer módulo 101 de circuito de conmutación y el segundo módulo 105 de circuito de conmutación están dispuestos en un circuito (chip) integrado común. En este caso, no tiene lugar una integración con el tercer módulo 201 de circuito de conmutación como funcionalidad de orden superior.

Por consiguiente, el primer módulo 101 de circuito de conmutación y el segundo módulo 105 de circuito de conmutación están incluidos en un circuito (chip) integrado común. Por lo tanto, se puede realizar un circuito integrado con una zona segura y una no segura.

La Fig. 8 muestra un diagrama esquemático de un equipo 200 de comunicaciones para la comunicación con un servidor de autenticación a través de una red de comunicaciones. El equipo 200 de comunicaciones de comunicaciones mostrado es una forma de realización posible del equipo 200 de comunicaciones de la Fig. 2.

El equipo 200 de comunicaciones comprende un sistema de identificación de abonado con un primer módulo 101 de circuito de conmutación y un segundo módulo 105 de circuito de conmutación, así como un tercer módulo 201 de circuito de conmutación. El primer módulo 101 de circuito de conmutación puede realizarse como módulo no seguro, el segundo módulo 105 de circuito de conmutación puede realizarse como módulo seguro y el tercer módulo 201 de circuito de conmutación puede realizar una funcionalidad de orden superior del equipo 200 de comunicaciones. El identificador de identidad de abonado es una Identidad Internacional del Abonado Móvil (IMSI).

El primer módulo 101 de circuito de conmutación, el segundo módulo 105 de circuito de conmutación y el tercer módulo 201 de circuito de conmutación como funcionalidad de orden superior, están dispuestos en un circuito (chip) integrado común. En este caso, no tiene lugar una integración con el tercer módulo 201 de circuito de conmutación como funcionalidad de orden superior.

Por consiguiente, el primer módulo 101 de circuito de conmutación, el segundo módulo 105 de circuito de conmutación y el tercer módulo 201 de circuito de conmutación como funcionalidad de orden superior, están incluidos en un circuito (chip) integrado común. En este caso, no tiene lugar una integración funcional.

De acuerdo con una forma de realización, el segundo módulo 105 de circuito de conmutación comprende adicionalmente el identificador de identidad de abonado o bien la IMSI. Las correspondientes funciones permiten la ejecución del algoritmo A, la escritura de la clave K criptográfica, así como la escritura y lectura del identificador de identidad de abonado o bien IMSI.

La Fig. 9 muestra un diagrama esquemático de un procedimiento 900 para la identificación de un abonado en una red de comunicaciones con utilización de un sistema de identificación de abonado. Al abonado están asociados un identificador de identidad de abonado y un calve criptográfica. El sistema de identificación de abonado comprende un primer módulo de circuito de conmutación con una primera interfaz de comunicaciones y un segundo módulo de circuito de conmutación con una segunda interfaz de comunicaciones, estando en el primer módulo de circuito de conmutación almacenado al menos el identificador de identidad de abonado y estando en el segundo módulo de circuito de conmutación almacenada al menos la clave criptográfica.

El procedimiento 900 comprende una recepción 901 de una señal de petición después del identificador de identidad de abonado mediante la primera interfaz de comunicaciones, en respuesta a la recepción de la señal de petición, un envío 903 del identificador de identidad de abonado mediante la primera interfaz de comunicaciones, una recepción 905 de un parámetro de entrada mediante la segunda interfaz de comunicaciones, una vinculación 907 del parámetro de entrada con la clave criptográfica con utilización de un algoritmo mediante el segundo módulo de circuito de conmutación, para obtener un parámetro de salida, y un envío 909 del parámetro de salida mediante la segunda interfaz de comunicaciones.

La Fig. 10 muestra un diagrama esquemático de un procedimiento 1000 para la comunicación con un servidor de autenticación a través de una red de comunicaciones con utilización de un equipo de comunicaciones. El equipo de comunicaciones comprende un sistema de identificación de abonado de acuerdo con la Fig. 1 y un tercer módulo de circuito de conmutación con una tercera interfaz de comunicaciones para la comunicación con el sistema de identificación de abonado y una cuarta interfaz de comunicaciones para la comunicación con el servidor de autenticación a través de la red de comunicaciones.

El procedimiento 1000 comprende un envío 1001 de la señal de petición al sistema de identificación de abonado mediante la tercera interfaz de comunicaciones, una recepción 1003 del identificador de identidad de abonado desde el sistema de identificación de abonado mediante la tercera interfaz de comunicaciones y un envío 1005 del identificador de identidad de abonado recibido al servidor de autenticación a través de la red de comunicaciones mediante la cuarta interfaz de comunicaciones.

Todas las características mostradas o descritas en relación con formas de realización individuales pueden estar previstas en cualquier combinación en el objeto de acuerdo con la invención para realizar al mismo tiempo sus efectos ventajosos.

Lista de símbolos de referencia

100	sistema de identificación de abonado
101	primer módulo de circuito de conmutación
103	primera interfaz de comunicaciones
105	segundo módulo de circuito de conmutación
107	segunda interfaz de comunicaciones
200	equipo de comunicaciones
201	tercer módulo de circuito de conmutación
203	tercera interfaz de comunicaciones
205	cuarta interfaz de comunicaciones
207	servidor de autenticación
209	red de comunicaciones
900	procedimiento para la identificación de un abonado en una red de comunicaciones
901	recepción de una señal de petición
903	envío del identificador de identidad de abonado
905	recepción de un parámetro de entrada
907	vinculación del parámetro de entrada con la clave criptográfica
909	envío del parámetro de salida
1000	procedimiento para la comunicación con un servidor de autenticación
1001	envío de la señal de petición
1003	recepción del identificador de identidad de abonado
1005	envío del identificador de identidad de abonado recibido

REIVINDICACIONES

1. Sistema (100) de identificación de abonado para la identificación de un abonado en una red (209) de comunicaciones, estando asociados al abonado un identificador de identidad de abonado y una clave (K) criptográfica, con:

un primer módulo (101) de circuito de conmutación, el cual está almacenado al menos el identificador de identidad de abonado, presentando el primer módulo (101) de circuito de conmutación una primera interfaz (103) de comunicaciones, la cual está configurada para recibir una señal de petición después del identificador de identidad de abonado y, en respuesta a la recepción de la señal de petición, enviar el identificador de identidad de abonado; y

un segundo módulo (105) de circuito de conmutación, en el cual está almacenada al menos la clave (K) criptográfica, presentado el segundo módulo (105) de circuito de conmutación una segunda interfaz (107) de comunicaciones, la cual está configurada para recibir un parámetro (I) de entrada, estando el segundo módulo (105) de circuito de conmutación configurado para vincular el parámetro (I) de entrada con la calve (K) criptográfica con utilización de un algoritmo (A) para obtener un parámetro (O) de salida, y estando la segunda interfaz (107) de comunicaciones configurada para enviar el parámetro (O) de salida;

estando el primer módulo (101) de conmutación y el segundo módulo (105) de conmutación dispuestos en un circuito integrado común.

2. Sistema (100) de identificación de abonado según la reivindicación 1, comprendiendo el primer módulo (101) de circuito de conmutación una primera memoria no volátil, estando almacenado al menos el identificador de identidad de abonado en la primera memoria no volátil, y comprendiendo el segundo módulo (105) de circuito de conmutación una segunda memoria no volátil, estando almacenada al menos la clave (K) criptográfica en la segunda memoria no volátil.

3. Sistema (100) de identificación de abonado según una de las reivindicaciones anteriores, comprendiendo el segundo módulo (105) de circuito de conmutación un circuito lógico, estando el circuito lógico configurado para vincular el parámetro (I) de entrada con la clave (K) criptográfica con utilización del algoritmo (A).

4. Sistema (100) de identificación de abonado según una de las reivindicaciones anteriores, formando el segundo módulo (105) de circuito de conmutación un módulo de seguridad hardware.

5. Sistema (100) de identificación de abonado según una de las reivindicaciones anteriores, siendo el identificador de identidad de abonado una Identidad Internacional del Abonado Móvil (IMSI).

6. Sistema (100) de identificación de abonado según una de las reivindicaciones anteriores, siendo el algoritmo (A) un algoritmo A3/A8, un algoritmo MILENAGE o un algoritmo TUAK.

7. Sistema (100) de identificación de abonado según una de las reivindicaciones anteriores, estando la clave (K) criptográfica almacenada de forma no legible en el segundo módulo (105) de circuito de conmutación.

8. Equipo (200) de comunicaciones para la comunicación con un servidor (207) de autenticación a través de una red (209) de comunicaciones, con:

un sistema (100) de identificación de abonado según una de las reivindicaciones 1 a 7; y

un tercer módulo (201) de circuito de conmutación con una tercera interfaz (203) de comunicaciones para la comunicación con el sistema (100) de identificación de abonado y una cuarta interfaz (205) de comunicaciones para la comunicación con el servidor (207) de autenticación a través de la red (209) de comunicaciones;

estando la tercera interfaz (203) de comunicaciones configurada para enviar la señal de petición al sistema (100) de identificación de abonado y recibir el identificador de identidad de abonado desde el sistema (100) de identificación de abonado; y

estando la cuarta interfaz (205) de comunicaciones configurada para enviar el identificador de identidad de abonado recibido al servidor (207) de autenticación a través de la red (209) de comunicaciones;

estando el primer módulo (101) de circuito de conmutación, el segundo módulo (105) de circuito de conmutación y el tercer módulo (201) de circuito de conmutación dispuestos en un circuito integrado común.

9. Equipo (200) de comunicaciones según la reivindicación 8, estando la cuarta interfaz (205) de comunicaciones además configurada para recibir el parámetro (I) de entrada desde el servidor (207) de autenticación a través de la red (209) de comunicaciones, estando la tercera interfaz (203) de comunicaciones además configurada para enviar el parámetro (I) de entrada al sistema (100) de identificación de abonado y recibir el parámetro (O) de salida desde el sistema (100) de identificación de abonado, y estando la cuarta interfaz (205) de comunicaciones además configurada para enviar el parámetro (O) de salida al servidor (207) de autenticación a través de la red (209) de comunicaciones.

10. Equipo (200) de comunicaciones según una de las reivindicaciones 8 o 9, comprendiendo el tercer módulo (201) de circuito de conmutación el primer módulo (101) de circuito de conmutación y/o el segundo módulo (105) de circuito de conmutación del sistema (100) de identificación de abonado.

11. Procedimiento (900) para la identificación de un abonado en una red (209) de comunicaciones con utilización de un sistema (100) de identificación de abonado, estando asociados al abonado un identificador de identidad de abonado y una clave (K) criptográfica, comprendiendo el sistema (100) de identificación de abonado un primer módulo (101) de circuito de conmutación con una primera interfaz (103) de comunicaciones y un segundo módulo (105) de circuito de conmutación con una segunda interfaz (107) de comunicaciones, estando en el primer módulo (101) de circuito de conmutación almacenado al menos el identificador de identidad de abonado, estando en el segundo módulo (105) de circuito de conmutación almacenada al menos la clave (K) criptográfica, estando el primer módulo (101) de circuito de conmutación y el segundo módulo (105) de circuito de conmutación dispuestos en un circuito integrado común, con:

recepción (901) de una señal de petición después del identificador de identidad de abonado mediante la primera interfaz (103) de comunicaciones;

en respuesta a la recepción de la señal de petición, envío (903) del identificador de identidad de abonado mediante la primera interfaz (103) de comunicaciones;

recepción (905) de un parámetro (I) de entrada mediante la segunda interfaz (107) de comunicaciones;

vinculación (907) del parámetro (I) de entrada con la clave (K) criptográfica con utilización de un algoritmo (A) mediante el segundo módulo (105) de circuito de conmutación para obtener un parámetro (O) de salida; y

envío (909) del parámetro (O) de salida mediante la segunda interfaz (107) de comunicaciones.

12. Procedimiento (1000) para la comunicación con un servidor (207) de autenticación a través de una red (209) de comunicaciones con utilización de un equipo (200) de comunicaciones, comprendiendo el equipo (200) de comunicaciones un sistema (100) de identificación de abonado según una de las reivindicaciones 1 a 7 y un tercer módulo (201) de circuito de conmutación con una tercera interfaz (203) de comunicaciones para la comunicación con el sistema (100) de identificación de abonado y una cuarta interfaz (205) de comunicaciones para la comunicación con el servidor (207) de autenticación a través de la red (209) de comunicaciones, estando el primer módulo (101) de circuito de conmutación, el segundo módulo (105) de circuito de conmutación y el tercer módulo (201) de circuito de conmutación dispuestos en un circuito integrado común, con:

envío (1001) de la señal de petición al sistema (100) de identificación de abonado mediante la tercera interfaz (203) de comunicaciones;

recepción (1003) del identificador de identidad de abonado desde el sistema (100) de identificación de abonado mediante a la tercera interfaz (203) de comunicaciones; y

envío (1005) del identificador de identidad de abonado recibido al servidor (207) de autenticación a través de la red (209) de comunicaciones mediante la cuarta interfaz (205) de comunicaciones.

13. Programa informático con un código de programa para la ejecución del procedimiento (900) según la reivindicación 11 o del procedimiento (1000) según la reivindicación 12.

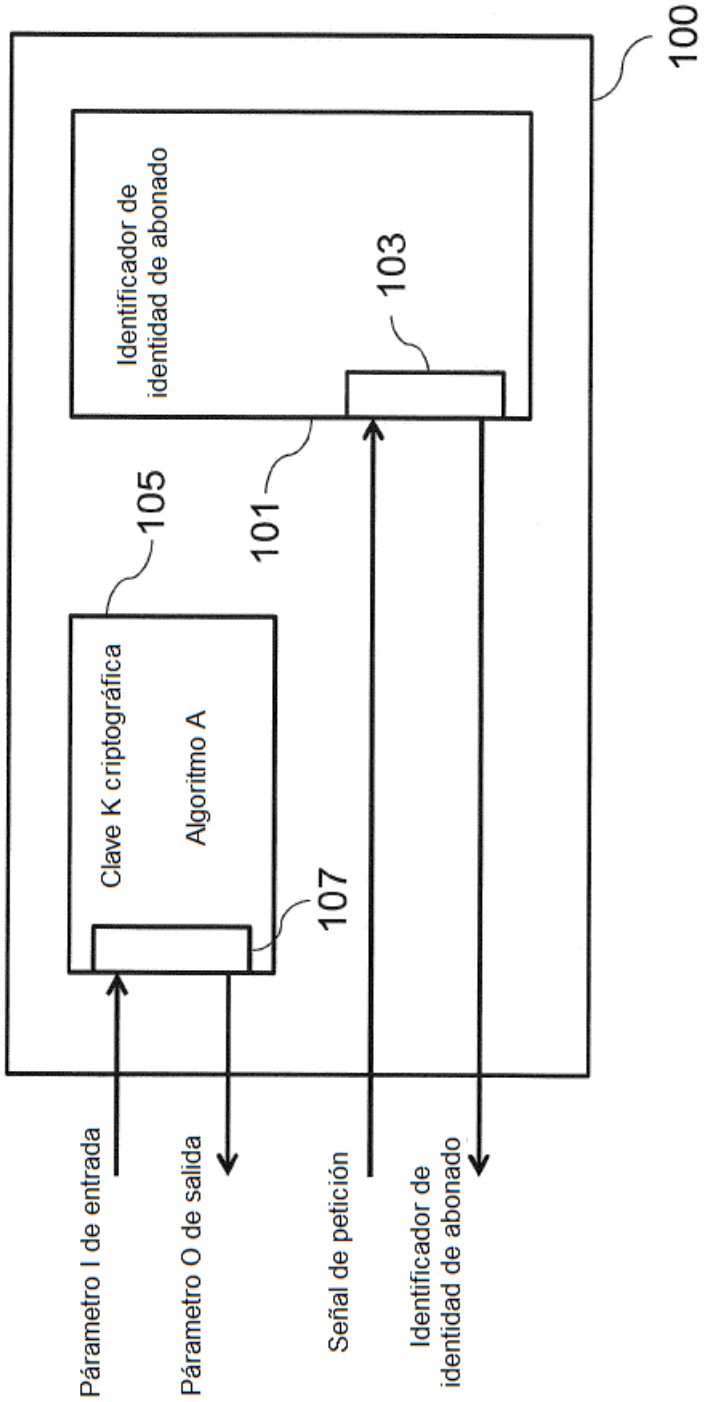
100
Identificador de identidad de abonado
103
101
105
Clave K criptográfica
Algoritmo A
107
Párametro I de entrada
Párametro O de salida
Señal de petición
Identificador de identidad de abonado

Fig. 1

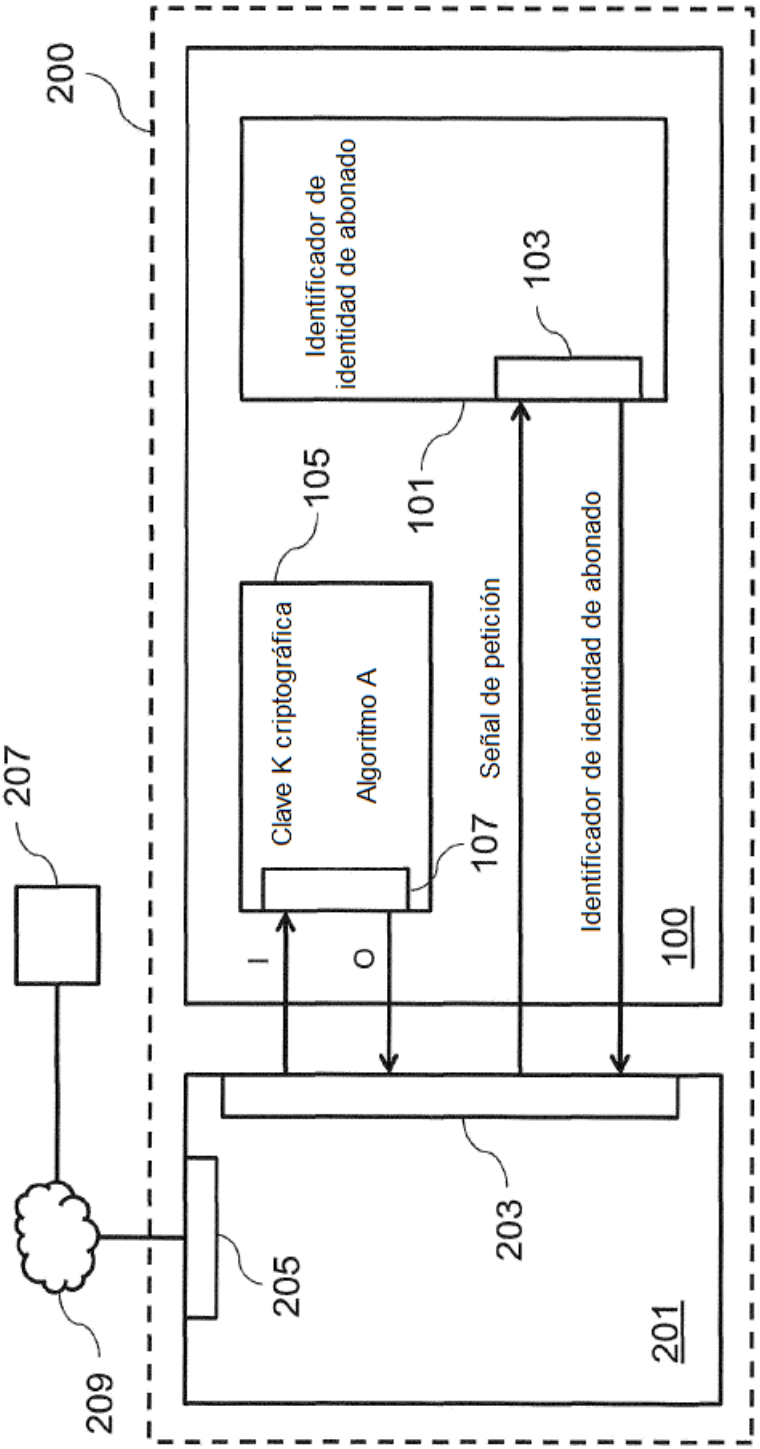
200
Identificador de identidad de abonado
103
101
105
Clave K criptográfica
Algoritmo A
107
Señal de petición
Identificador de identidad de abonado
100
I
O
207
203
205
201
209

Fig. 2

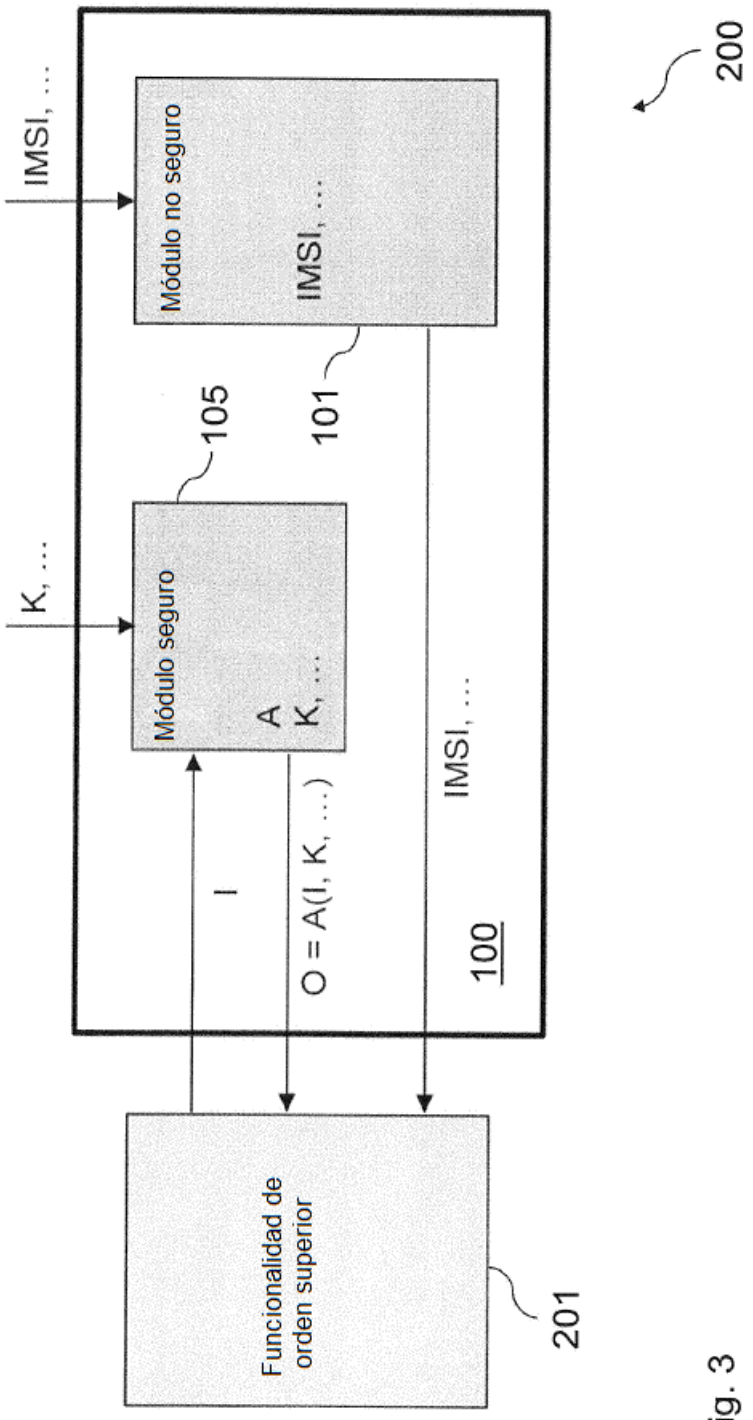
IMSI, ...
Módulo no seguro
IMSI, ...
200
105
101
K, ...
Módulo seguro
A
K, ...
I
O = A(I, K, ...)
IMSI, ...
100
Funcionalidad de orden superior
201

Fig. 3

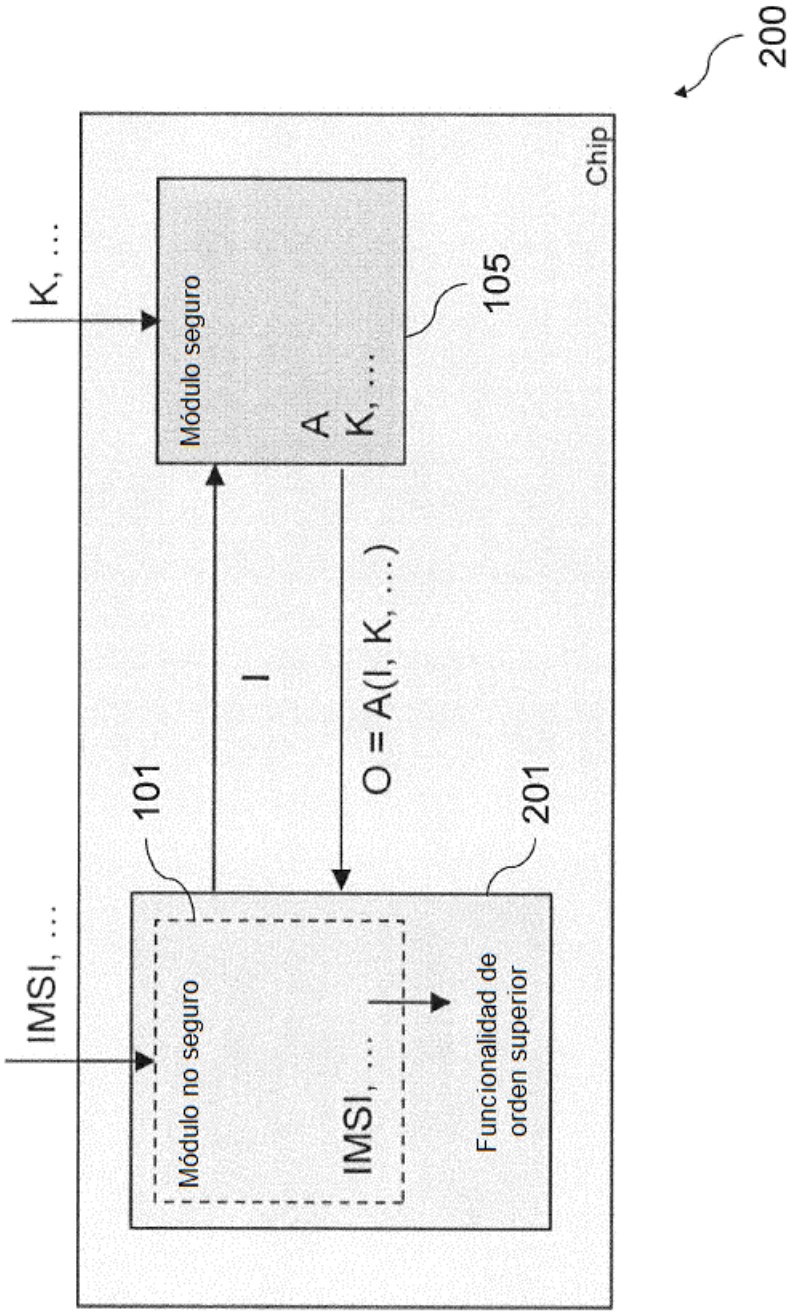
200
Chip
K, ...
Módulo seguro
A
K, ...
105
I
O = A(I, K, ...)
101
201
IMSI, ...
Módulo no seguro
IMSI, ...
Funcionalidad de orden superior

Fig. 4

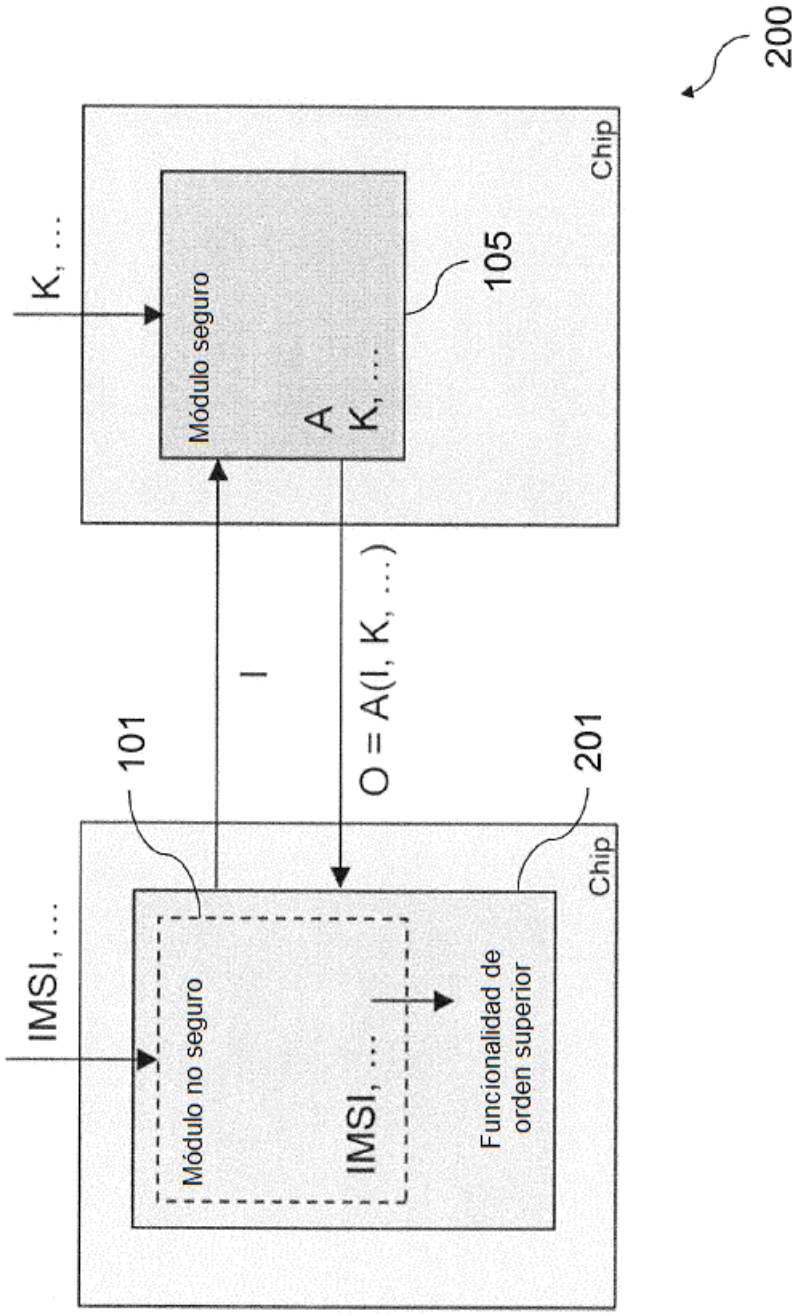
200
Chip
K, ...
Módulo seguro
A
K, ...
105
I
O = A(I, K, ...)
101
201
Chip
IMSI, ...
Módulo no seguro
IMSI, ...
Funcionalidad de orden superior

Fig. 5

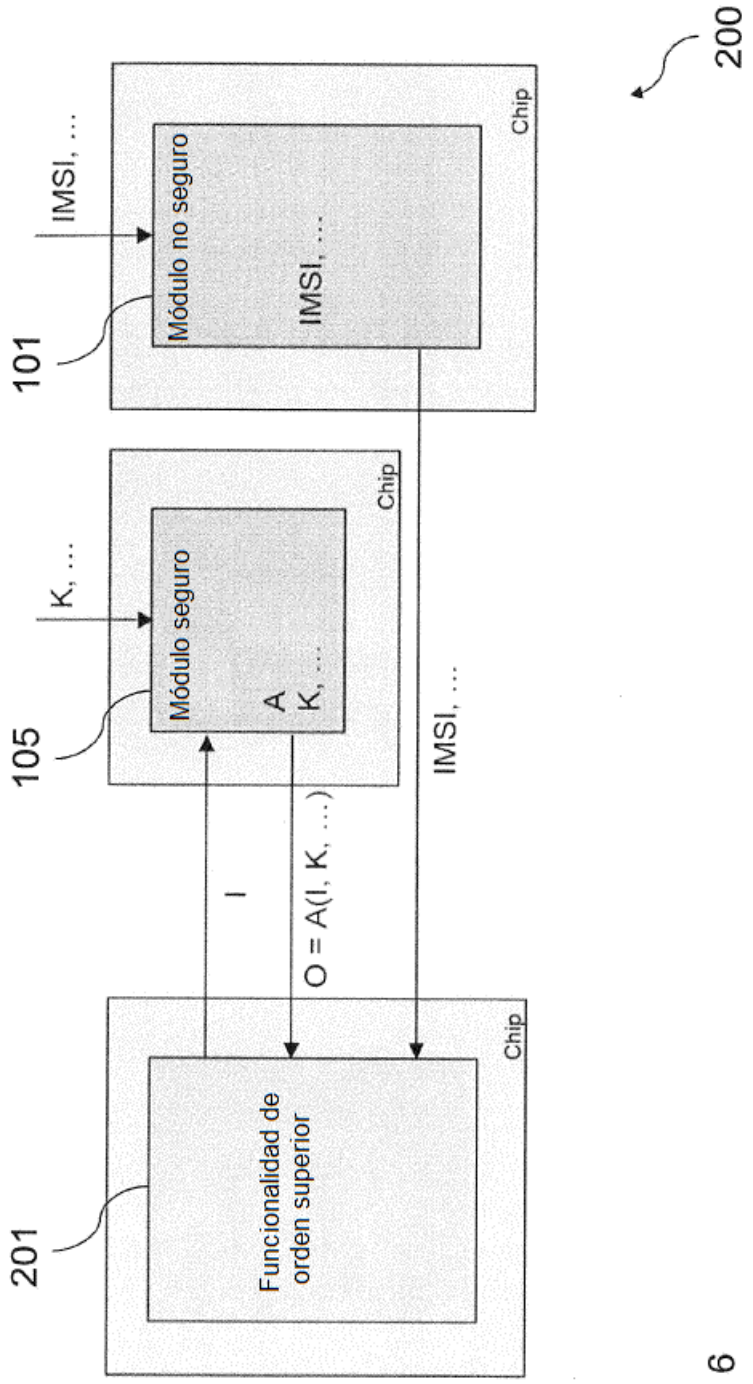
200
Chip
IMSI, ...
Módulo no seguro
IMSI, ...
101
Chip
K, ...
Módulo seguro
A
K, ...
105
IMSI, ...
I
O = A(I, K, ...)
Chip
Funcionalidad de orden superior
201

Fig. 6

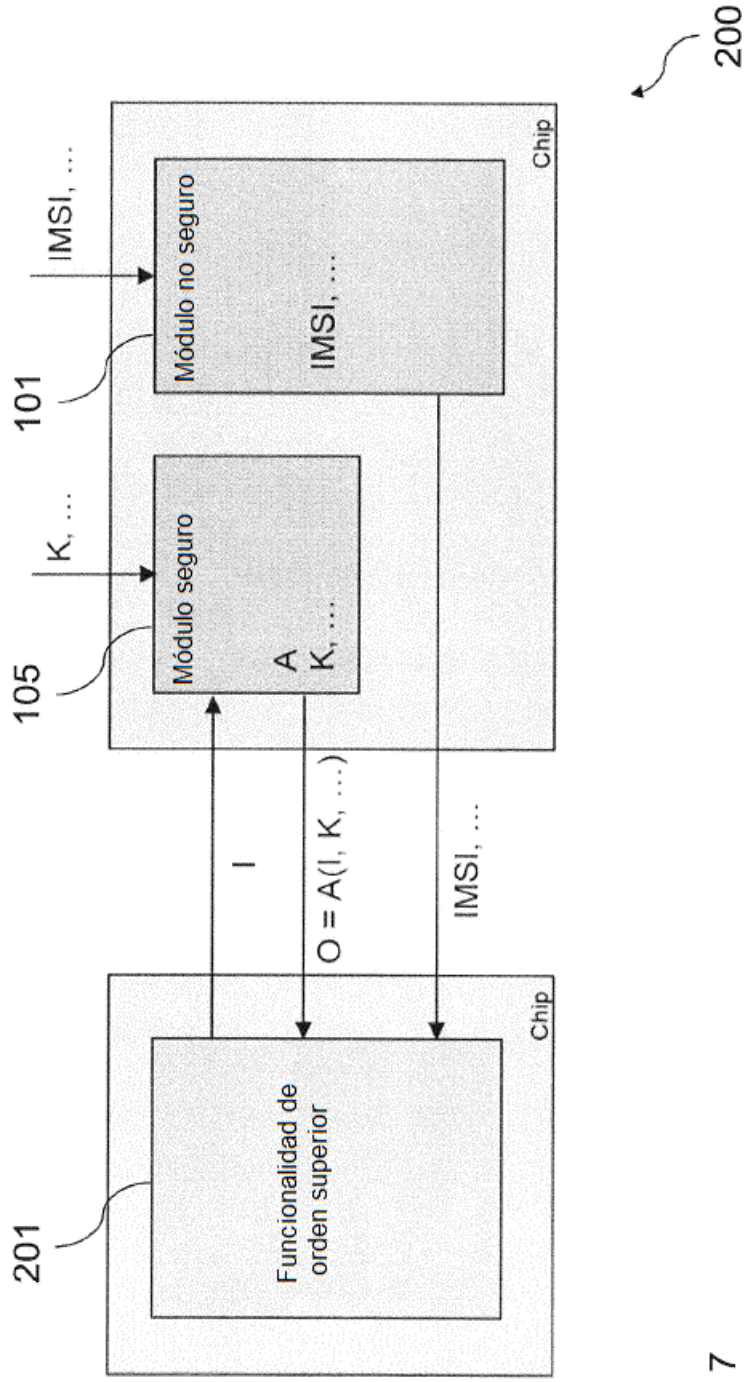
200
Chip
IMSI, ...
101
Módulo no seguro
IMSI, ...
K, ...
105
Módulo seguro
A
K, ...
I
O = A(I, K, ...)
IMSI, ...
Chip
201
Funcionalidad de orden superior

Fig. 7

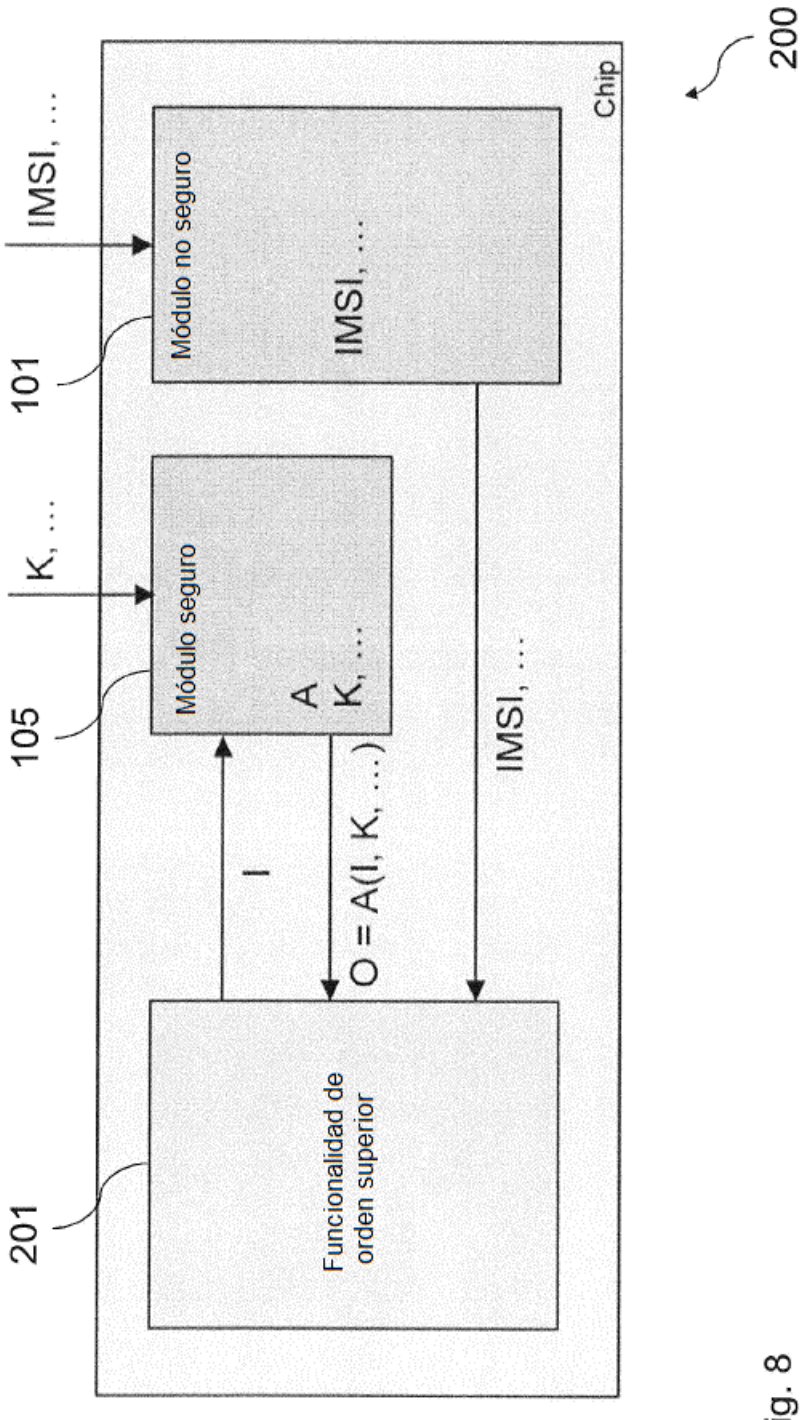
200
Chip
IMSI, ...
101
Módulo no seguro
IMSI, ...
K, ...
105
Módulo seguro
A
K, ...
I
O = A(I, K, ...)
IMSI, ...
201
Funcionalidad de orden superior

Fig. 8

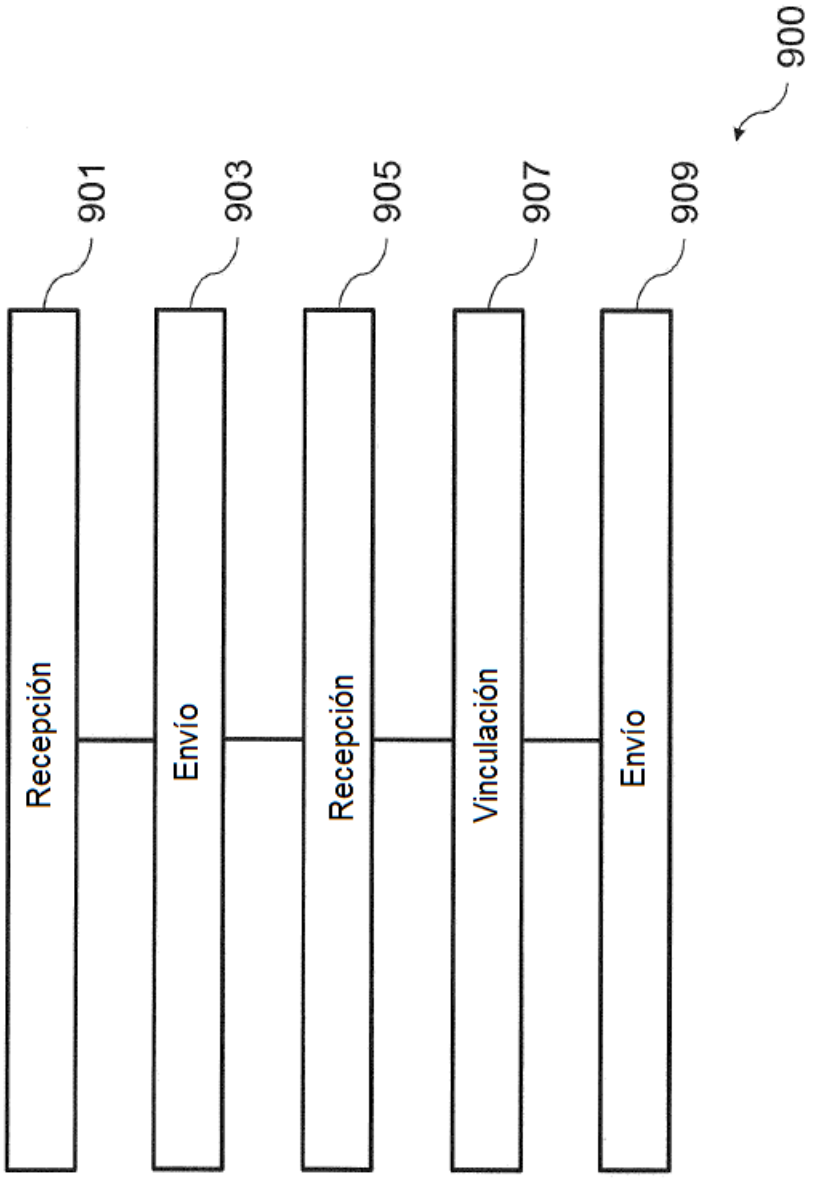
900
901
903
905
907
909
Recepción
Envío
Recepción
Vinculación
Envío

Fig. 9

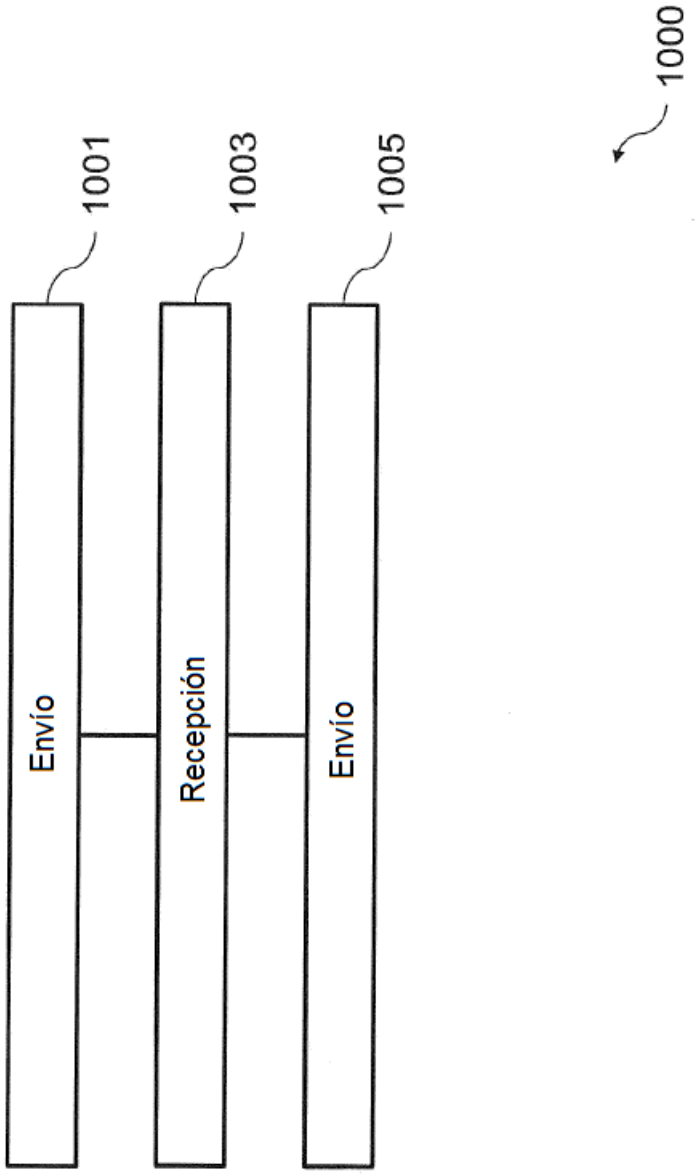

Fig. 10