(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 279 868**

(51) Int. Cl.:
H04Q 7/38 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
H04Q 7/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **02737051 .9**
(86) Fecha de presentación : **21.05.2002**
(87) Número de publicación de la solicitud: **1396169**
(87) Fecha de publicación de la solicitud: **10.03.2004**

(54) Título: **Autenticación local en un sistema de comunicación.**

(30) Prioridad: **22.05.2001 US 863139**

(45) Fecha de publicación de la mención BOPI:
01.09.2007

(45) Fecha de la publicación del folleto de la patente:
01.09.2007

(73) Titular/es: **QUALCOMM INCORPORATED**
5775 Morehouse Drive
San Diego, California 92121-1714, US

(72) Inventor/es: **Quick, Roy, F., Jr. y**
Rose, Gregory, G.

(74) Agente: **Carpintero López, Francisco**

DESCRIPCIÓN

Autenticación local en un sistema de comunicación.

Antecedentes

I. Campo de la invención

La presente invención se refiere a sistemas de comunicación, y de manera más particular, a la autenticación local de un abonado del sistema de comunicación.

II. Antecedentes

El campo de las comunicaciones inalámbricas presenta muchas aplicaciones incluyendo, por ejemplo, teléfonos inalámbrico, sistemas de mensajería (paging), bucles locales inalámbricos, asistentes digitales personales (PDA's), telefonía por Internet, y sistemas de comunicación por satélite. Una aplicación particularmente importante son los sistemas de telefonía móvil para abonados móviles. Tal como se utiliza en el presente documento, el término sistema "móvil" engloba tanto frecuencias de servicios de comunicaciones móviles como personales (PCS). Diversas interfaces sobre el aire se han desarrollado para este tipo de sistemas de telefonía móvil incluyendo, por ejemplo, el acceso múltiple por división de frecuencia (FDMA), acceso múltiple por división de tiempo (TDMA), y acceso múltiple por división por código (CDMA). En conexión con lo mismo, se han establecido diversas normas nacionales e internacionales incluyendo, por ejemplo, el servicio telefónico móvil avanzado (advanced mobile phone service (AMPS)), sistema global para móviles (global system for mobile (GSM)), y la norma provisional (Interim Standard (IS-95)). En particular, la IS-95 y sus derivados, la IS-95A, IS-95B, la ANSI J-STD-008 (a las que a menudo se hará referencia colectivamente como IS-95 en el presente documento), y sistemas de tasa de datos alta propuestos para datos, etc. se promulgan por la asociación de industria de las telecomunicaciones (telecommunication industry association (TIA)) y otros cuerpos de normas bien conocidos.

Los sistemas de telefonía móvil configurados según la utilización de la norma IS-95 emplean técnicas de procesamiento de señal CDMA para proporcionar un servicio de telefonía móvil altamente eficiente y firme. Los sistemas de telefonía móvil a modo de ejemplo configurados sustancialmente según la utilización de la norma IS-95 se describen en la patente de los EE.UU. Nº 5.103.459 y 4.901.307.

Un sistema a modo de ejemplo que utiliza las técnicas CDMA es la propuesta de tecnología de transmisión de radio cdma2000 ITU-R (a la que se hace referencia en el presente documento como cdma2000), publicado por la TIA. La norma para el cdma2000 se proporciona en las versiones del borrador de la IS-2000 y la TIA lo ha aprobado. La propuesta cdma2000 es compatible con los sistemas IS-95 en muchas maneras. Otra norma CDMA es la norma W-CDMA, tal como se realiza en el proyecto conjunto de tercera generación (3rd Generation Partnership Project) "·3GPP", con número de documento 3G TS 25.211, 3G TS 25.212, 3G TS 25.213 y 3G TS 25.214.

Dada la omnipresente proliferación de servicios de telecomunicaciones en la mayor parte del mundo y el incremento de movilidad de la población en general, se desea proporcionar servicios de comunicación a un abonado mientras él o ella viaja fuera del alcance del sistema doméstico del abonado. Un procedimiento para satisfacer esta necesidad es la utilización de un testigo (token) de identificación, tal como el módulo de identificación del abonado (subscriber identity module (SIM)) en sistemas GSM, en los que se asigna a un abonado un tarjeta SIM que puede introducirse en un teléfono GSM. La tarjeta SIM lleva información que se utiliza para identificar la información de facturación de la parte que introduce la tarjeta SIM en un teléfono móvil. A la siguiente generación de tarjetas SIM se le dado el nuevo nombre de tarjetas USIM (UTMS SIM). En un sistema CDMA, al testigo de identificación se hace referencia como módulo de interfaz de usuario desmontable (removable user interface (R-UIM)) y consigue la misma finalidad. La utilización de este tipo de testigo de identificación permite a un abonado viajar sin su teléfono móvil personal, que puede configurarse para funcionar en frecuencias que se utilizan en el entorno que se visita, y utilizar un teléfono móvil disponible localmente sin incurrir en los costes del establecimiento de una nueva cuenta.

Aunque conveniente, la utilización de este tipo de testigos de identificación para acceder a la información de la cuenta de un abonado puede ser insegura. Comúnmente, este tipo de testigos de identificación se programan para transmitir información privada, tal como una clave criptográfica que se utiliza para codificar mensajes o una clave de autenticación para identificar al abonado, al teléfono móvil. Una persona que contempla la posibilidad del robo de la información de una cuenta puede conseguir su propósito mediante la programación de un teléfono móvil para quedarse con la información privada después de que el testigo de identificación se haya eliminado, o transmitir información privada a otra unidad de almacenamiento durante la utilización legítima del teléfono móvil. A los teléfonos móviles que se han falsificado de esta manera se hará referencia de ahora en adelante como "cuerpos invasores". Por tanto, hay una necesidad vigente de preservar la seguridad de la información privada almacenada en un testigo de identificación mientras aun se facilita la utilización de dicha información privada para acceder a los servicios de comunicación.

"Rouges MS_Shell Treat Analysis" 3GPP TSG SA WG3 SECURITY, [Online] del 28 de noviembre de 2000 (28-11-2000), al 30 noviembre de 2000 (30-11-2000) páginas 1 a 17, XP002210348 Sophia Antipolis, Francia, describe un módulo de identificación de abonado que comprende: un elemento de generación de clave; y un generador de firmas configurado para recibir una clave secreta del elemento de generación de clave e información desde una unidad

móvil y configurar adicionalmente para emitir una firma a la unidad móvil. Desde el módulo de identificación de abonado conocido por este documento la firma se genera utilizando una función criptográfica genérica. La firma en este momento se dirige de vuelta a la unidad móvil dejando información/datos privados vulnerables de ser atacados si la unidad móvil es un elemento malicioso.

Sumario

Se presenta un procedimiento y aparato novedosos para proporcionar autenticación segura a un abonado en itinerancia (roaming) fuera de su sistema doméstico.

En un aspecto se proporciona un dispositivo de identificación de abonado según la reivindicación 1.

En otro aspecto, se presenta un procedimiento para proporcionar la autenticación de un abonado utilizando un dispositivo de identificación de abonado según la reivindicación 12.

Descripción detallada de los dibujos

La figura 1 es un diagrama de un sistema de comunicación de datos a modo de ejemplo.

La figura 2 es un diagrama de un intercambio de comunicación entre los componentes en un sistema de comunicación inalámbrico.

La figura 3 es un diagrama de una realización en la que un testigo de identificación de abonado proporciona un soporte de codificación a una unidad móvil.

La figura 4 es un diagrama de una realización en la que una función de “hash” (direccionamiento calculado) se utiliza para generar una firma de autenticación.

La figura 5 es un diagrama de flujo de un procedimiento para direccionar un mensaje con el fin de generar una firma de autenticación.

Descripción detallada de las realizaciones

Tal como se ilustra en la figura 1, una red 10 de comunicación inalámbrica generalmente incluye una pluralidad de estaciones 12a - 12d móviles (también denominadas unidades del abonado o equipo del usuario), una pluralidad de estaciones 14a - 14c base (también denominadas transceptores de estación base (BTS) o nodo B), un controlador de estación base (BSC) (también denominado controlador de red de radio o función 16 de control de paquetes), un centro de conmutación móvil (MSC) o conmutador 18, un nodo de servicio de paquetes de datos (PDSN) o función 20 de internetfuncionamiento (IWF), una red 22 telefónica pública conmutada (PSTN) (normalmente una compañía telefónica), y una red 24 de protocolo de Internet (IP) (normalmente Internet). Para simplificar, se muestran cuatro estaciones 12a - 12b móviles, tres estaciones 14a - 14c base, un BSC 16, un MSC 18, y un PDSN 20. Los expertos en la técnica entenderán que puede haber cualquier número de estaciones 12 móviles, estaciones 14 base, BSC 16, MSC 18, y PDSN 20.

En una realización, la red 10 de comunicación inalámbrica es una red de servicios de paquetes de datos. Las estaciones 12a - 12b móviles pueden ser cualquiera de un número de diferentes tipos de dispositivos de comunicación inalámbrica tal como un teléfono portátil, un teléfono móvil que está conectado a un ordenador portátil con procesos basada en IP, aplicaciones de navegador de web, un teléfono móvil para automóviles con kits de manos libres asociado, un asistente de datos personal (PDA) con procesos basados en IP, aplicaciones de navegador de web, un módulo de comunicación inalámbrica incorporado a un ordenador portátil, o módulo de comunicación de localización fija tal como puede encontrarse en un bucle local inalámbrico o un sistema de lectura de medidor. En la realización más general, las estaciones móviles pueden ser cualquier tipo de unidad de comunicación.

Las estaciones 12a - 12b móviles pueden configurarse para realizar uno o más protocolos de paquetes de datos inalámbricos tales como, por ejemplo, la norma EIA/TIA/IS-707. En una realización particular, las estaciones 12a - 12b móviles generan paquetes IP destinados para la red 24 IP y encapsulan los paquetes IP en tramas utilizando el protocolo punto a punto (PPP).

En una realización la red 24 IP se acopla al PDSN 20, el PDSN 20 se acopla al MSC 18, el MSC 18 se acopla al BSC 16 y a la PSTN 22, y el BSC 16 se acopla a las estaciones 14a - 14b base a través de líneas alámbricas configuradas para la transmisión de paquetes de datos y/o voz según cualquiera de los diversos protocolos conocidos incluyendo, por ejemplo, E1, T1, modo de transferencia asíncrona (Asynchronous Transfer Mode (ATM)), IP, retransmisión de trama, HDSL; ADSL, o xDSL. En una realización alternativa, el BSC 16 se acopla directamente al PDSN 20, y el MSC no se acopla al PDSN 20. En otra realización de la invención, las estaciones 12a - 12d móviles se comunican con las estaciones 14a - 14c base a través de una interfaz RF definida en el proyecto conjunto de tercera generación 2 “3GPP2”, “Physical Layer Standard for cdma2000 Spread Spectrum Systems,” 3GPP2 en el documento Nº C.P0002-A, TIA PN-4694, que se publicará como TIA/EIA/IS-2000-2-A, (Borrador, versión editada 30) (19 de noviembre de1999).

Durante el funcionamiento normal de una red 10 de comunicación inalámbrica, las estaciones 14a -14c base reciben y demodulan conjuntos de señales de enlace inverso de diversas estaciones 12a - 12d móviles acopladas en llamadas telefónicas, navegaciones de web, u otras comunicaciones de datos. Cada señal de enlace inverso recibida a través de una estación 14a - 14c base dada se procesa dentro de esa estación 14a - 14c base. Cada estación 14a - 14c base puede comunicarse con una pluralidad de estaciones 12a -12d móviles mediante la modulación y transmisión de conjuntos de señales de enlace directo a las estaciones 12a -12d móviles. Por ejemplo, tal como se muestra en la figura 1, la estación 14a base se comunica con la primera y segunda estación 12a, 12b móvil simultáneamente, y la estación 14c base se comunica con una tercera y cuarta estación 12c, 12d móvil simultáneamente. Los paquetes resultantes se envían al BSC 16, que proporciona asignación de recursos de llamada y funcionalidad de gestión de movilidad incluyendo la organización de traspasos continuos de una llamada para una estación 12a - 12d móvil particular desde una estación 14a - 14c base a otra estación 14a - 14c base. Por ejemplo, una estación 12c móvil está comunicando con dos estaciones 14b, 14 c base de manera simultánea. Finalmente, cuando la estación 12c móvil se desplaza suficientemente lejos de una de las estaciones 14c base, la llamada se traspasará a la otra estación 14b base.

Si la transmisión es una llamada de teléfono convencional, el BSC 16 encaminará los datos recibidos al MSC 18, que proporciona servicios de encaminamiento adicionales para la interfaz con la PSTN 22. Si la transmisión es una transmisión basada en paquetes tal como una llamada de datos destinada a la red 24 IP, el MSC 18 encaminará los paquetes de datos al PDSN 20, que enviará los paquetes a la red 24 IP. Alternativamente, el BSC 16 encaminará los paquetes directamente al PSDN 20, que envía los paquetes a la red 24 IP.

La figura 2 ilustra un procedimiento para autenticar a un abonado utilizando un teléfono móvil en un sistema de comunicación inalámbrico. Un abonado que viaja fuera del alcance de su sistema 200 domestico (Home System (HS)) utiliza una unidad 220 móvil en un sistema 210 visitado (Visited System (VS)). El abonado utiliza la unidad 220 móvil insertando un testigo de identificación del abonado. Un testigo de identificación del abonado de este tipo se configura para generar información de codificación y de autenticación que permite a un abonado acceder a los servicios de cuenta sin la necesidad de establecer una nueva cuenta con el sistema visitado. Una petición (no se muestra en la figura) se envía desde la unidad 220 móvil al VS 210 para tener servicio. El VS 210 contacta con el HS 200 para determinar el servicio al abonado (no se muestra en la figura).

El HS 200 genera un número 240 aleatorio y una respuesta 270 esperada (Expected Response (XRES)) basada en el conocimiento de la información privada guardada en el testigo de identificación de abonado. El número 240 aleatorio se utilizará como un desafío, en el que el receptor de destino utiliza el número 240 aleatorio y el conocimiento privado para generar una respuesta de confirmación que coincide con la respuesta 270 esperada. El número 240 aleatorio y la XRES 270 se transmiten desde el HS 200 al VS 210. También se transmite otra información, pero no es tan relevante para este documento (no se muestra en la figura). La comunicación entre el HS 200 y el VS 210 se facilita de la manera descrita en la figura 1. El VS 210 transmite el número 240 aleatorio a la unidad 220 móvil y espera la transmisión de un mensaje 260 de confirmación de la unidad 220 móvil. El mensaje 260 de confirmación y la XRES 270 se comparan en un elemento 280 de comparación en el VS 210. Si el mensaje 260 de confirmación y la XRES 270 coinciden, el VS 210 procede a proporcionar servicio a la unidad 220 móvil.

La unidad 220 móvil envía el número 240 aleatorio al testigo 230 de identificación de abonado que el abonado ha insertado dentro de la unidad 220 móvil. Una clave 300 de seguridad se almacena en el testigo 230 de identificación de abonado. Tanto la clave 300 de seguridad como el número 240 aleatorio se utilizan mediante un generador 250 de clave para generar el mensaje 260 de confirmación, una clave 290 de codificación (Cipher Key (CK)), y una clave 310 de integridad (Integrity Key (IK)). La CK 290 y la IK 310 se transportan a la unidad 220 móvil.

En la unidad 220 móvil, la CK 290 puede utilizarse para codificar comunicaciones entre la unidad 220 móvil y el VS 210, de manera que las comunicaciones puedan decodificarse sólo mediante el receptor destinado del mensaje. Las técnicas para la utilización de una clave criptográfica para codificar comunicaciones se describen en la patente de los EE.UU. Nº 649035 titulada, “Method and Apparatus for Generating Encryption Stream Cypher” (Procedimiento y aparato para la generación de cifrados de flujo codificados), transferida al cesionario de la presente invención. Otras técnicas de codificación pueden utilizarse sin afectar al alcance de las realizaciones descritas en el presente documento.

La IK 310 puede utilizarse para generar un código de autenticación de mensaje (MAC), en el que se agrega el MAC a una trama de mensaje de transmisión para verificar que la trama de mensaje de transmisión se originó desde una parte en especial y para verificar que el mensaje no se alteró durante la transmisión. Las técnicas para generar los MAC se describen en el documento WO0111818 titulado, “Method and Apparatus for Generating a Message Authentication Code” (Procedimiento y aparato para generar un código de autenticación de mensaje). Otras técnicas para generar códigos de autenticación pueden utilizarse sin afectar al alcance de las realizaciones descritas en el presente documento. Por tanto, el término “firma” como se utiliza en el presente documento representa la salida de cualquier esquema de autenticación que puede implementarse en un sistema de comunicación.

De manera alternativa, la KI 310 puede utilizarse para generar una firma 340 de autenticación basada en la información particular que se transmite de manera separada o junto con el mensaje de transmisión. Las técnicas para generar una firma de autenticación se describen en la patente de los EE.UU. 5.943.615, titulada “Method and Apparatus for Providing Authentication Security in a Wireless Communication System” (Procedimiento y aparato para proporcionar seguridad de autenticación en un sistema de comunicación inalámbrico), trasferida al cesionario de la presente invención. La firma 340 de autenticación es la salida de un elemento 330 de direccionamiento calculado que combina la IK

310 con un mensaje 350 desde la unidad 220 móvil. La firma 340 de autenticación y el mensaje 350 se transmiten por el aire al VS 210.

Tal como se observa en la figura 2, la clave 290 criptográfica y la clave 310 de integridad se transmiten desde el testigo 230 de identificación de abonado a la unidad 220 móvil, que procede a generar tramas de datos para la propagación pública por el aire. Aunque esta técnica puede impedir que una persona que intercepta mensajes determine los valores de este tipo de claves por el aire, esta técnica no proporciona protección del ataque de un cuerpo malicioso. Un cuerpo malicioso puede programarse para aceptar la CK 290 y la IK 310, y a continuación almacenar las claves en lugar de purgar la presencia de claves de este tipo de la memoria local. Otro procedimiento para robar claves es programar la unidad 220 móvil para transmitir claves recibidas a otra localización. La CK 290 y la IK 310 pueden facturar de manera fraudulenta comunicaciones no autorizadas al abonado. Este ataque de cuerpo malicioso es particularmente efectivo en sistemas en los que el número aleatorio generado en el sistema 200 doméstico se utiliza de una manera que es insegura, tal como el caso cuando las mismas claves generadas se utilizan durante un periodo de tiempo extenso.

Una realización que protege contra un ataque de cuerpos maliciosos utiliza los procesadores y la memoria en el testigo de identificación de abonado para generar una firma electrónica que no puede reproducirse mediante una unidad móvil sin la introducción del testigo de identificación del abonado.

La figura 3 ilustra una realización para la realización de la autenticación local de un abonado en un sistema de comunicación inalámbrico. En esta realización, se programa el testigo 230 de identificación de abonado para generar una respuesta de autenticación basada en una clave que no se pasa a la unidad 220 móvil. Por tanto, si la unidad móvil utilizada por un abonado es un cuerpo malicioso, el cuerpo malicioso no puede recrear las respuestas de autenticación apropiadas.

De manera similar al procedimiento descrito en la figura 2, la unidad 220 móvil genera una señal de firma basada en una IK 310 que se recibe del testigo 230 de identificación de abonado y un mensaje que debe enviarse al VS 210. Sin embargo, en una realización, la señal de firma no se pasa al VS. La señal de firma se pasa al testigo 230 de identificación de abonado, y se utiliza junto con una clave adicional para generar una señal de firma primaria. La señal de firma primaria se envía a la unidad 220 móvil, que a su vez transmite la señal de firma primaria al VS 210 para fines de autenticación.

El HS 200 genera un número 240 aleatorio y una respuesta 270 esperada (XRES) en base al conocimiento de la clave de seguridad mantenida en el testigo 230 de identificación de abonado. El número 240 aleatorio y la XRES 270 se transmiten al VS 210. La comunicación entre el HS 200 y el VS 210 se facilita de la manera descrita en la figura 1. El VS 210 transmite el número 240 aleatorio a la unidad 220 móvil y espera la transmisión de un mensaje 260 de confirmación de la unidad 220 móvil. El mensaje 260 de confirmación y la XRES 270 se comparan en un elemento 280 de comparación en el VS 210. Si el mensaje 260 de confirmación y la XRES 270 coinciden, el VS 210 procede a proporcionar servicio a la unidad 220 móvil.

La unidad 220 móvil transporta el número 240 aleatorio al testigo 230 de identificación de abonado que el abonado ha acoplado electrónicamente con la unidad 220 móvil. Una 300 de seguridad se almacena en el testigo 230 de identificación de abonado. Un generador 250 de claves utiliza tanto la clave 300 de seguridad como el número 240 aleatorio para generar el mensaje 260 de confirmación, una clave 290 codificada (CK), una clave 310 de integridad (IK), y una clave 320 de autenticación UIM (UAK). La CK 290 y la IK 310 se transportan a la unidad 220 de móvil.

En la unidad 220 móvil, se utiliza la CK 290 para codificar tramas de datos de transmisión (no se muestra en la figura 3). La IK 310 se utiliza para generar una señal 340 se firma. La señal 340 de firma es la salida de un generador 330 de firmas que utiliza una operación de codificación o una operación unidireccional, tal como una función de direccionamiento calculado, de la IK 310 y un mensaje 350 desde la unidad 220 móvil. La señal 340 de firma se transmite al testigo 230 de identificación de abonado. En el testigo 230 de identificación de abonado un generador 360 de firmas manipula la señal 340 de firma y la UAK 320 para generar una señal 370 de firma primaria. La señal 370 de firma primaria se transmite a la unidad 220 móvil y al VS 210, en los que un elemento 380 de verificación autentica la identidad del abonado. El elemento 380 de verificación puede conseguir la verificación volviendo a generar la señal 340 de firma y la señal 370 de firma primaria. Alternativamente, el elemento 380 de verificación puede recibir la señal 340 de firma desde la unidad 220 móvil y volver a generar sólo la señal 370 de firma primaria.

La regeneración de la señal 340 de firma y la señal 370 de firma primaria en el VS 210 puede conseguirse mediante una diversidad de técnicas. En una realización, el elemento 380 de verificación puede recibir una UAK 390 y una clave de integridad desde el sistema 200 doméstico. Cuando el elemento 380 de verificación también recibe el mensaje 350 desde la unidad 220 móvil, puede generarse la señal de firma y posteriormente utilizarse para generar el elemento de firma primario.

El generador 360 de firmas en el testigo 230 de identificación de abonado puede comprender una memoria y un procesador, en el que el procesador puede configurarse para manipular entradas utilizando una diversidad de técnicas. Estas técnicas pueden adoptar la forma de técnicas de codificación, funciones de direccionamiento calculado, o cualquier operación no reversible. Como ejemplo, una técnica que el testigo de identificación de abonado puede implementar es el algoritmo de direccionamiento calculado seguro, (SHA), divulgado en la Norma de Procesamiento de Información Federal (FIPS) PUB 186, “Norma de firma digital” (“Digital Signature Standard”), mayo 1994. Otra

técnica que el testigo de identificación de abonado puede llevar a cabo es la Norma de Codificación de Datos (Data Encryption Standard (DES)), divulgada en FIPS PUB 46, enero 1977. La utilización del término "codificación" tal como se utiliza en el presente documento no implica necesariamente que las operaciones tengan que ser reversibles. Las operaciones pueden ser no reversibles en las realizaciones descritas en el presente documento.

El generador 250 de claves puede comprender también una memoria y un procesador. De hecho, en una realización, puede configurarse un único procesador para conseguir las funciones del generador 360 de firmas y el generador 250 de claves. La verificación puede llevarse a cabo calculando el mismo resultado de las mismas entradas en el elemento 380 de verificación, y comparando los valores calculados y transmitidos.

En una descripción más detallada de la realización anterior, puede configurarse el generador 330 de señales para implementar una técnica a la que se hace referencia en el presente documento como HMAC-SHA-1. En la realización descrita anteriormente, se observó que podía utilizarse una función de direccionamiento calculado en el generador 330 de señales para generar una señal 340 de firma. Una descripción de MAC basados en direccionamiento calculado (HMAC) puede encontrarse en el documento, "Keying Hash Functions for Message Authentication" (Funciones de direccionamiento calculado de clave para la autenticación de mensajes), Bellare, *et al*., Advances in Cryptology-Crypto 96 Proceedings, Lecture Notes in Computer Science Vol. 1109, Springer - Verlag, 1996. Un HMAC es un esquema MAC que utiliza una función de direccionamiento calculado codificada, tal como SHA-1, en un proceso de dos etapas. En un esquema HMAC-SHA-1, una clave aleatoria y secreta inicializa la función SHA-1, que entonces se utiliza para producir un resumen del mensaje. Luego se utiliza la clave para inicializar otra vez el SHA-1 para producir un resumen del primer resumen. Este segundo resumen proporciona un MAC que se adjuntará a cada mensaje. En la realización descrita en el presente documento, puede utilizarse la clave 310 de integridad (IK) que genera el testigo 230 de identificación de abonado como la clave aleatoria y secreta que inicializa el SHA-1. La figura 4 es un diagrama de flujo que ilustra la implementación del HMAC en la estación móvil, que se inicializa mediante una clave de integridad del testigo de identificación de abonado, y la implementación del HMAC en el testigo de identificación de abonado, que se inicializa mediante una clave de autenticación UIM.

En la figura 4, el HS 200 genera un número 240 aleatorio y una respuesta 270 esperada (XRES) en base al conocimiento de la información privada mantenida en el testigo 230 de identificación de abonado. El número 240 aleatorio y la XRES 270 se transmiten al VS 210. La comunicación entre el HS 200 y el VS 210 se facilita de la manera descrita en la figura 1. El VS 210 transmite el número 240 aleatorio a la unidad 220 móvil y espera la transmisión de un mensaje 260 de confirmación desde la unidad 220 móvil. El mensaje 260 de confirmación y la XRES 270 se comparan en un elemento 280 de comparación en el VS 210. Si el mensaje 260 de confirmación y la XRES 270 coinciden, el VS 210 procede a proporcionar servicio a la unidad 220 móvil.

La unidad 220 móvil transporta el número 240 aleatorio al testigo 230 de identificación de abonado que el abonado ha acoplado electrónicamente con la unidad 220 móvil. Una clave 300 de seguridad se almacena en el testigo 230 de identificación de abonado. Un generador 250 de claves utiliza tanto la clave 300 de seguridad como el número 240 aleatorio para generar el mensaje 260 de confirmación, una clave 290 codificada (CK), una clave 310 de integridad (IK), y una clave 320 de autenticación UIM (UAK). La CK 290 y la IK 310 se transportan a la unidad 220 móvil.

En la unidad 220 móvil, se utiliza la CK 290 para codificar tramas de datos de transmisión (no se muestra en la figura 4). La IK 310 se utiliza para generar una señal 340 de firma del generador 330 de firmas. El generador 330 de firmas se configura para producir una transformación del mensaje 260 a través de la utilización del SHA-1. La IK 310 inicializa la función de direccionamiento calculado del SHA-1

La señal 340 de firma, que es el resultado de la función de direccionamiento calculado SHA-1 que transforma el mensaje 260, se transmite al testigo 230 de identificación de abonado. En el testigo 230 de identificación de abonado, la señal 340 de firmas y la UAK 320 se manipulan por medio de un generador 360 de firmas para generar una transformación de la señal 340 de firma, que es el código 370 (UMAC) de autenticación de mensaje UIM. El generador 360 de firmas se configura también para implementar la función de direccionamiento calculado SHA-1. Sin embargo, la función se inicializa utilizando UAK 320, en lugar de la IK 310.

El UMAC 370 se transmite a la unidad 220 móvil y al VS 210, en el que un elemento 380 de verificación autentica la identidad del abonado. El elemento 380 de verificación puede llevar a cabo la verificación regenerando la señal 340 de firma y el UMAC 370. Alternativamente, el elemento 380 de verificación puede recibir la señal 340 de firma desde la unidad 220 móvil y solamente regenerar el UMAC 370.

La figura 5 es un diagrama de flujo que ilustra una descripción generalizada de la realización. En la etapa 500, una unidad móvil genera un mensaje que requiere autenticación. En la etapa 501, la unidad móvil recibe una clave (IK) de integridad de longitud L de un testigo de identificación de abonado. En la etapa 502, la unidad móvil rellena la clave IK de integridad hasta la longitud b, en la que b es el tamaño de bloque de la función de direccionamiento calculado de un generador de firmas dentro de la unidad móvil. En una realización, la clave puede rellenarse de ceros hasta la longitud b. En otra realización, a la clave puede aplicarse una operación XOR con constantes de relleno de longitud b. Si la KI ya tiene longitud b, puede omitirse esta etapa. En la etapa 504, la IK rellenada se concatena al mensaje que requiere autenticación. La concatenación de la IK rellenada y el mensaje se dispersa entonces en la etapa 505 mediante un generador de firmas configurado para implementar una función de direccionamiento calculado tal como la SHA. En una realización, la salida de la operación XOR se guarda dentro de un elemento de memoria, y puede volverse a

llamar para su utilización posterior si la IK del testigo de identificación del abonado sigue siendo el mismo durante la sesión de comunicación.

Si va a utilizarse la clave (UAK) de autenticación UIM, entonces el flujo de programa avanza hasta la etapa 510. Si no va a utilizarse la UAK, entonces el flujo de programa avanza hasta la etapa 520.

En la etapa 510, el mensaje dispersado de la etapa 505 se transmite al testigo de identificación de abonado. En la etapa 511, el testigo de identificación de abonado rellena la UAK hasta longitud b, a menos que la UAK ya sea de longitud b. La IK rellenada puede almacenarse en la memoria para reutilizarse cuando un mensaje posterior requiera autenticación durante la sesión de comunicación. En la etapa 512, la IK rellenada y el mensaje dispersado se concatenan y se introducen en un generador de firmas. El generador de firmas se configura para implementar una función de direccionamiento calculado, tal como la SHA-1 en la etapa 513. En la etapa 514, la salida del generador de firmas se transmite desde el testigo de identificación de abonado a la unidad móvil.

En la etapa 520, la misma clave de integridad se utiliza para volver a direccionar el mensaje ya dispersado. El mensaje dispersado de la etapa 505 se envía a un segundo generador de firmas dentro de la unidad móvil. O como alternativa, el mensaje dispersado puede reinsertarse en el generador de firmas de la etapa 505. Si una clave de integridad va a utilizarse en dos procesos de direccionamiento calculado, entonces debe alterarse la clave de integridad de tal manera que cada uno de los generadores de direccionamiento calculado se inicializa con un valor diferente. Por ejemplo, para cada etapa de direccionamiento calculado, la clave de integridad puede añadirse a nivel de bit a o bien el valor c_1 constante o valor c_2 constante, ambos de longitud b. Utilizando este procedimiento, solo una de las claves de integridad necesita generarse mediante el testigo de identificación de abonado.

Debe observarse que la realización más segura es la implementación en la que la segunda etapa de direccionamiento calculado se lleva a cabo utilizando la UAK en el testigo de identificación de abonado.

El proceso descrito en la figura 5 puede describirse matemáticamente mediante la ecuación:

$$HMAC(x) = F_{testigo}(UAK, F_{móvil}(IK, x)),$$

en la que $F_Y(\ )$ representa una función de direccionamiento calculado realizada en una ubicación Y, x representa el mensaje original, UAK e IK son las claves, y una coma representa la concatenación.

Un testigo de identificación de usuario utilizado en un sistema CDMA o un sistema GSM, también conocidos como un R-UIM o USIM, respectivamente, puede configurarse para generar la señal de firma primaria o UMAC de la forma descrita anteriormente, es decir, todos los mensajes generados por la unidad móvil se codifican y autentican. Sin embargo, puesto que la unidad de procesamiento central en dichos testigos puede limitarse, puede desearse implementar una realización alternativa, en la que un peso de importancia se asigna a una trama de mensaje de tal manera que sólo se codifican y autentican de manera segura mensajes importantes. Por ejemplo, una trama de mensaje que contiene información de facturación tiene más necesidad de aumentar la seguridad que una trama de mensaje que contiene una carga útil de voz. Por tanto, la unidad móvil puede asignar un mayor peso de importancia a la trama de mensaje de información de facturación y un menor peso de importancia a la trama de mensaje de voz. Cuando el testigo de identificación de abonado recibe las señales de firma generadas a partir de estos mensajes pesados, la CPU puede evaluar los diferentes pesos de importancia unidos a cada señal de firma y determina una señal de firma primaria para solamente las señales de firma de mucho peso. Como alternativa, la unidad de comunicación puede programarse para transportar sólo las señales de firma "importantes" al testigo de identificación de abonado. Este procedimiento de generación selectiva de señales de firma primarias aumenta la eficacia del testigo de identificación de abonado mediante el aligeramiento de la carga de procesamiento al testigo de identificación de abonado.

Las realizaciones descritas anteriormente impiden la utilización no autorizada de una cuenta de abonado al requerir una transacción más segura entre el testigo de identificación de abonado y la unidad móvil. Puesto que la unidad móvil no puede generar una señal de firma primaria sin conocer la UAK secreta, la unidad móvil que se programa para actuar como un cuerpo malicioso no puede apropiarse indebidamente de la información del abonado para fines improcedentes.

Las realizaciones descritas anteriormente también maximizan la capacidad de procesamiento del testigo de identificación de abonado operando sobre una señal de firma, en lugar de un mensaje. Normalmente, una señal de firma tendrá una longitud de bits más corta que un mensaje. Por tanto, se requiere menos tiempo para que el generador de firmas en la identificación de abonado para operar sobre una señal de firma en lugar de una trama de mensaje de transmisión. Tal como se menciona anteriormente, la capacidad de procesamiento del testigo de identificación de abonado es por lo general mucho menor que la capacidad de procesamiento de la unidad móvil. Por tanto, la implementación de esta realización proporcionaría autenticación de seguridad de mensajes sin sacrificar la velocidad.

Sin embargo, debe observarse que se producen mejoras en arquitecturas del procesador a un ritmo casi exponencial. Realizaciones de este tipo consisten en tiempos de procesamiento más rápidos y tamaños menores del procesador. Por tanto, puede implementarse otra realización para proporcionar autenticación local, en la que la señal de firma primaria puede generarse directamente a partir de un mensaje, en lugar de indirectamente a través de una señal de firma corta.

Una unidad móvil puede configurarse para pasar un mensaje directamente al testigo de identificación de abonado, uno con la capacidad para generar una señal de firma primaria rápidamente, en lugar de pasar el mensaje a un elemento de generación de firmas dentro de la unidad móvil. En otra realización, sólo un número limitado de mensajes necesita pasarse directamente al testigo de identificación de abonado, según el grado de seguridad que se necesite para dichos mensajes.

Debe observarse que mientras se han descrito varias realizaciones en el contexto de un sistema de comunicación inalámbrico, las diversas realizaciones pueden utilizarse además para proporcionar autenticación local segura de cualquier parte utilizando un terminal desconocido conectado en una red de comunicaciones.

Así, se han descrito procedimientos y aparatos mejorados y novedosos para llevar a cabo autenticación local de un abonado en un sistema de comunicación. Aquellos expertos en la técnica entenderían que las diversas etapas de algoritmos, circuitos, módulos, y bloques lógicos ilustrativas descritas en relación a las realizaciones dadas a conocer en el presente documento pueden implementarse como hardware electrónico, software, firmware, o combinaciones de los mismos. Los diversos componentes ilustrativos, bloques, módulos, circuitos y etapas se han descrito generalmente en términos de su funcionalidad. Si la funcionalidad se implementa como hardware, software, o como firmware depende de la aplicación particular y las limitaciones de diseño impuestas sobre la totalidad del sistema. Los expertos en la técnica admiten la intercambiabilidad de hardware, software y firmware bajo estas circunstancias, y como implementar mejor la funcionalidad descrita para cada aplicación particular.

La implementación de diversas etapas de algoritmos, circuitos, módulos, y bloques lógicos descritas en relación con las realizaciones dadas a conocer en el presente documento pueden implementarse o llevarse a cabo con un procesador de señales digitales (“Digital Signal Processor ” (DSP)), un circuito integrado específico de la aplicación (“Application Specific Integrated Circuit ” (ASIC)), una matriz de puertas programable *in situ*, (“Field Programmable Gate Array” (FPGA)) u otro dispositivo de lógica programable, componentes de hardware discretos, de lógica de transistor o puerta discreta. Un procesador que ejecuta un conjunto o instrucciones de firmware, cualquier módulo de software programable convencional y un procesador, o una combinación de los mismos puede diseñarse para llevar a cabo las funciones descritas en el presente documento. El procesador puede ser, de manera ventajosa, un microprocesador, pero como alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador, o máquina de estado convencional. El módulo de software podría residir en la memoria RAM, memoria flash, memoria ROM, memoria EPROM, memoria EEPROM, registradores, disco duro, disco extraíble, CD-ROM, o cualquier otra forma de medio de almacenamiento conocido en la técnica. Un procesador a modo de ejemplo se acopla al medio de almacenamiento para leer información de, y escribir información al, medio de almacenamiento. Como alternativa, el medio de almacenamiento puede residir en un ASIC. El ASIC puede residir en un teléfono u otro terminal de usuario. Como alternativa, el procesador y el medio de almacenamiento pueden residir en un teléfono u otro terminal de usuario. El procesador puede implementarse como una combinación de un DSP y un microprocesador, o como dos microprocesadores junto con un núcleo DSP, etc. Aquellos expertos apreciarían adicionalmente que los datos, instrucciones, comandos, información, señales, bits, símbolos y chips a los que puede hacerse referencia en toda la descripción anterior se representasen mediante voltajes, corrientes, ondas electromagnéticas, partículas o campos magnéticos, partículas o campos ópticos, o cualquier combinación de los mismos.

Así, se han mostrado y descrito las diversas realizaciones de la presente invención. Resultará obvio a cualquier experto en la técnica común, sin embargo, que pueden hacerse numerosas modificaciones a las realizaciones dadas a conocer en el presente documento sin apartarse del alcance de la invención.

REIVINDICACIONES

1. Un dispositivo (230) de identificación de abonado para proporcionar autenticación local de un abonado en un sistema de comunicación, que comprende:

medios para la generación de una pluralidad de claves (290, 310, 320) en respuesta a un desafío recibido;

medios para la generación de un valor inicial basado en una primera clave (320) de la pluralidad de claves; y para

la concatenación del valor inicial con una señal (340) recibida para formar una firma de entrada, en el que la señal (340) recibida se transmite desde una unidad (220) de comunicación que funciona en un sistema acoplado de forma comunicativa al dispositivo (230) de identificación de abonado, y la señal (340) recibida se genera mediante la unidad (220) de comunicación utilizando una segunda clave (310) de la pluralidad de claves, habiéndose comunicado la segunda clave (310) desde el dispositivo (230) de identificación de abonado a la unidad (220) de comunicación;

medios de direccionamiento calculado de la firma de entrada para formar una firma (370) de autenticación; y

medios para la transmisión de la firma (370) de autenticación al sistema de comunicación a través de la unidad (220) de comunicación.

2. Dispositivo de identificación de abonado según la reivindicación 1, en el que los medios de direccionamiento calculado se adaptan para direccionar la firma de entrada según el algoritmo de direccionamiento calculado seguro, SHA-1.

3. Dispositivo de identificación de abonado según la reivindicación 1, en el que los medios para la generación del valor inicial se adaptan para rellenar la primera clave.

4. Dispositivo de identificación de abonado según la reivindicación 3, en el que los medios para la generación del valor inicial se adaptan adicionalmente para añadir la primera clave rellenada a nivel de bit a un valor constante.

5. Dispositivo de identificación de abonado según la reivindicación 1, en el que la unidad (220) de comunicación se adapta para generar la señal (340) recibida mediante;

la recepción de la segunda clave (310) desde el dispositivo (230) de identificación de abonado;

la generación de un valor inicial local basado en la segunda clave;

la concatenación del valor inicial local y un mensaje para formar un valor de entrada local;

el direccionamiento calculado del valor de entrada local para formar la señal (340) recibida; y

la transmisión de la señal (340) recibida al dispositivo de identificación de abonado.

6. Dispositivo de identificación de abonado según la reivindicación 5, en el que la generación del valor inicial local comprende rellenar la segunda clave.

7. Dispositivo de identificación de abonado según la reivindicación 6, en el que la generación del valor inicial local comprende además la adición de la segunda clave rellenada a nivel de bit a un segundo valor constante.

8. Dispositivo de identificación de abonado según cualquiera de las reivindicaciones anteriores que comprende:

una memoria; y

un procesador configurado para implementar un conjunto de instrucciones almacenadas en la memoria,

en el que dicho procesador comprende:

dichos medios para la generación de una pluralidad de claves;

dichos medios para la generación y concatenación del valor inicial; y

dichos medios de direccionamiento calculado de la firma de entrada.

9. Dispositivo de identificación de abonado según una cualquiera de las reivindicaciones 1 a 7 en el que:

los medios para la generación de una pluralidad de claves comprenden

un elemento (250) de generación de claves, y

dicho dispositivo de identificación de abonado comprende además un generador (360) de firmas,

comprendiendo dicho generador (360) de firmas dichos medios para la generación del valor inicial y para la concatenación del valor inicial con una señal recibida y dichos medios de direccionamiento calculado.

10. Dispositivo de identificación de abonado según la reivindicación 9, en el que el elemento (250) de generación de claves comprende:

una memoria; y

un procesador configurado para ejecutar un conjunto de instrucciones almacenadas en la memoria, en el que el conjunto de instrucciones realiza una transformación criptográfica de un valor de entrada para producir una pluralidad de claves temporales.

11. Módulo de identificación de abonado según la reivindicación 10, en el que la transformación criptográfica se realiza utilizando una clave permanente.

12. Un procedimiento para proporcionar la autenticación de un abonado utilizando un dispositivo (230) de identificación de abonado, que comprende:

generar una pluralidad de claves (290, 310, 320);

transmitir una segunda clave (310) de la pluralidad de claves a una unidad (220) de comunicación en un sistema de comunicación acoplado de forma comunicativa al dispositivo (230) de identificación de abonado y mantener privada la primera clave (320) de la pluralidad de claves;

generar una firma (340) en la unidad (220) de comunicación utilizando tanto la segunda clave (310) transmitida a la unidad de comunicación como un mensaje de transmisión, en el que la generación se implementa mediante el direccionamiento calculado de un valor concatenado formado de la segunda clave (310) y el mensaje de transmisión;

transmitir la firma (340) al dispositivo (230) de identificación de abonado;

recibir la firma (340) en el dispositivo (230) de identificación de abonado;

generar en el dispositivo (230) de identificación de abonado una firma (370) de autenticación de la firma (340) recibida, en el que la generación se implementa mediante el direccionamiento calculado de un valor concatenado formado de la primera clave (320) y la firma (340) recibidas de la unidad (220) de comunicación; y

transportar la firma (370) de autenticación al sistema de comunicación.

13. Procedimiento según la reivindicación 12, en el que el direccionamiento calculado se implementa según el SHA-1.

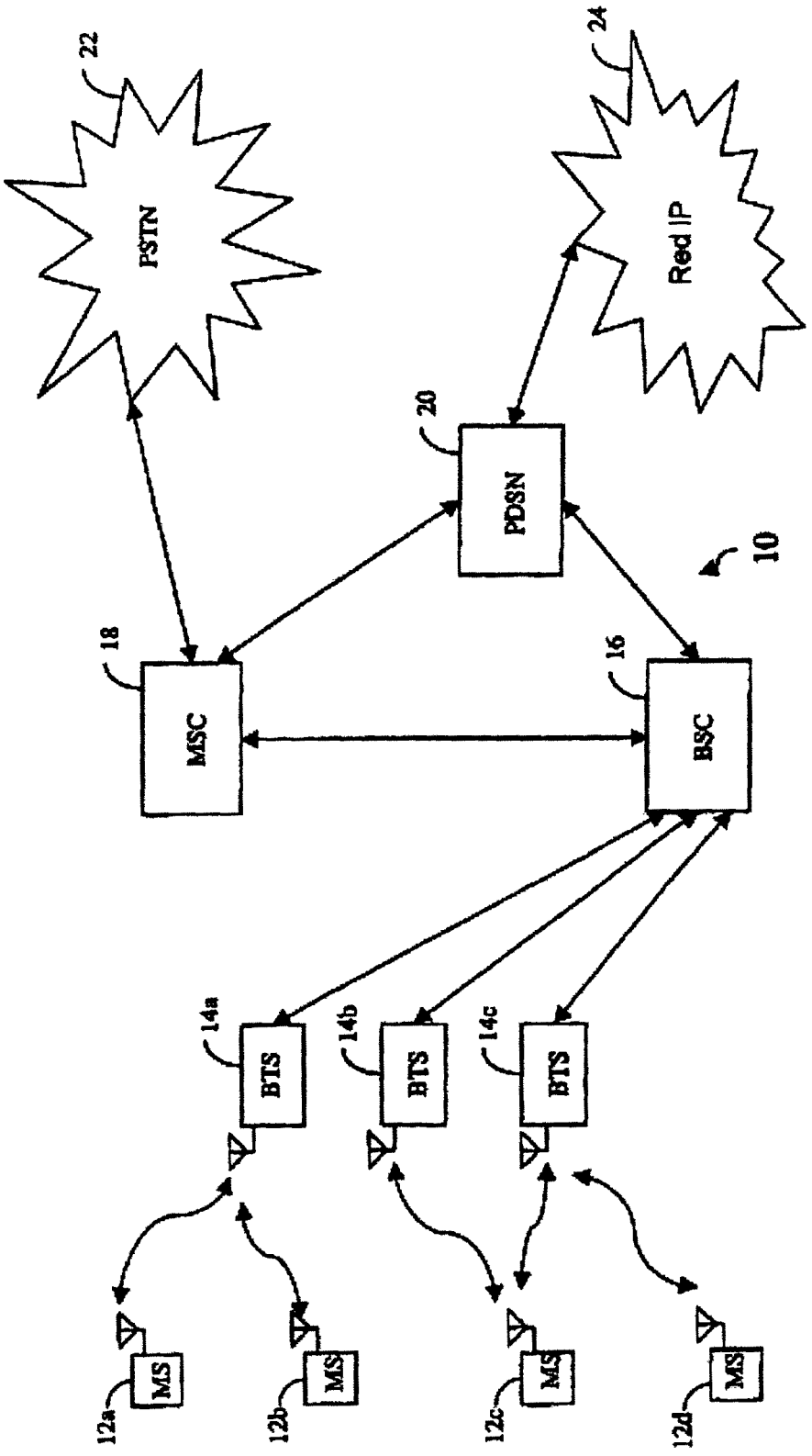
22
PSTN
24
Red IP
20
PDSN
10
18
MSC
16
BSC
14a
BTS
14b
BTS
14c
BTS
MS
12a
MS
12b
MS
12c
MS
12d

FIG. 1

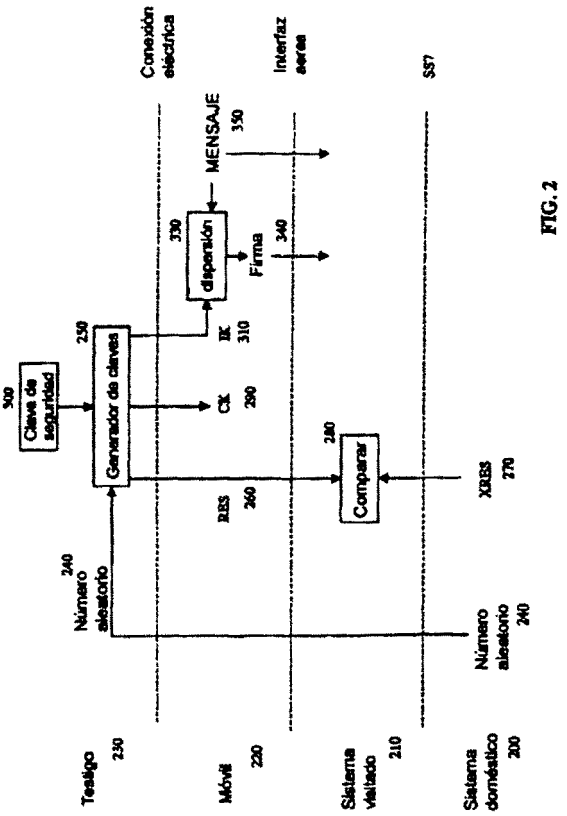
Conexión eléctrica
Interfaz aérea
SS7
MENSAJE
350
dispersión
330
Firma
340
Clave de seguridad
309
Generador de claves
250
IK
310
CK
290
RES
260
Comparar
280
XRES
270
Número aleatorio
240
Número aleatorio
240
Testigo
230
Móvil
220
Sistema velado
210
Sistema doméstico
200

FIG. 2

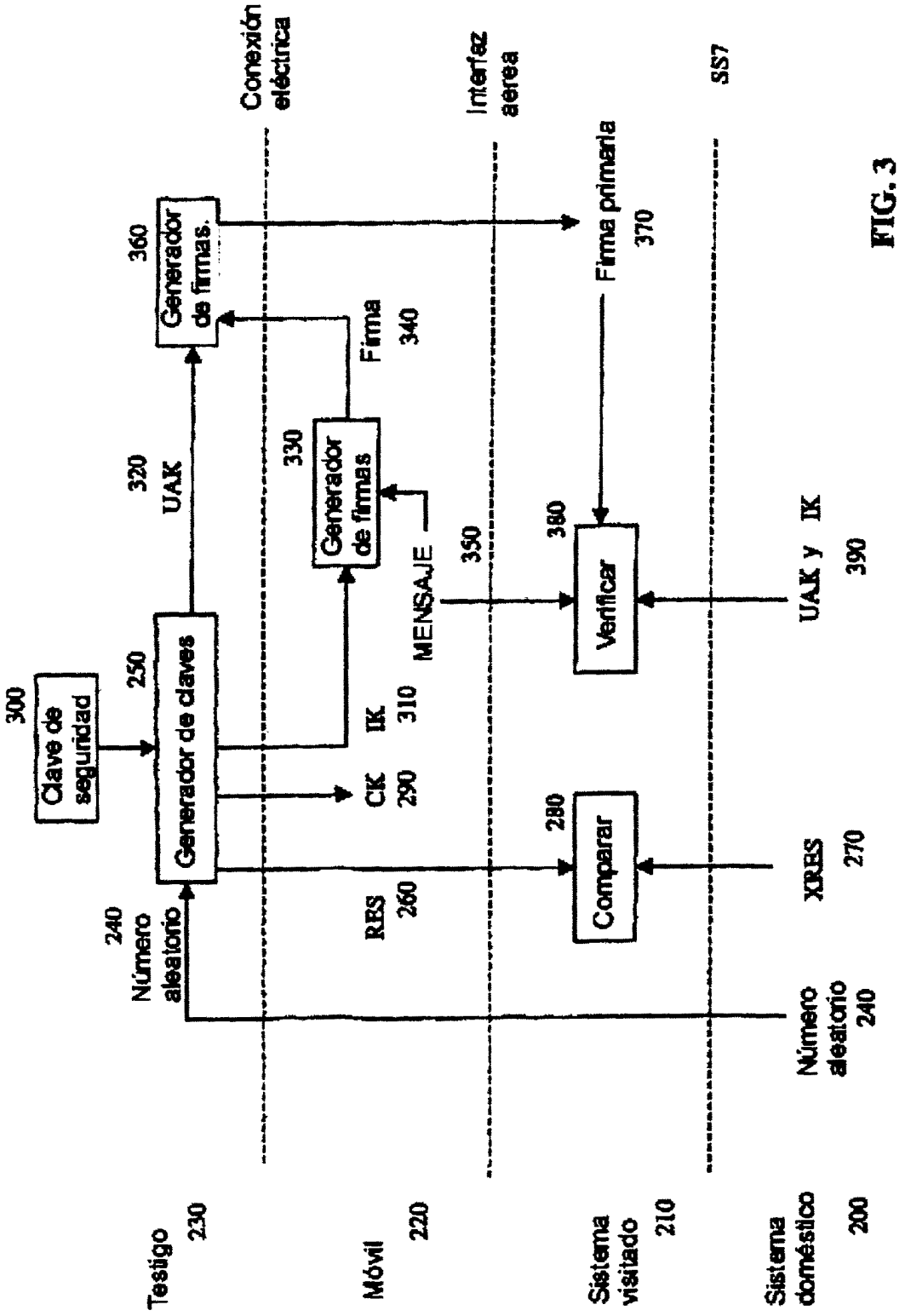
Conexión eléctrica
Interfaz aérea
SS7
Clave de seguridad
300
Generador de claves
250
Generador de firmas.
360
Generador de firmas
330
UAK
320
IK
310
CK
290
Firma
340
Firma primaria
370
MENSAJE
350
Verificar
380
UAK y IK
390
Comparar
280
RES
260
XRES
270
Número aleatorio
240
Número aleatorio
240
Testigo
230
Móvil
220
Sistema visitado
210
Sistema doméstico
200

FIG. 3

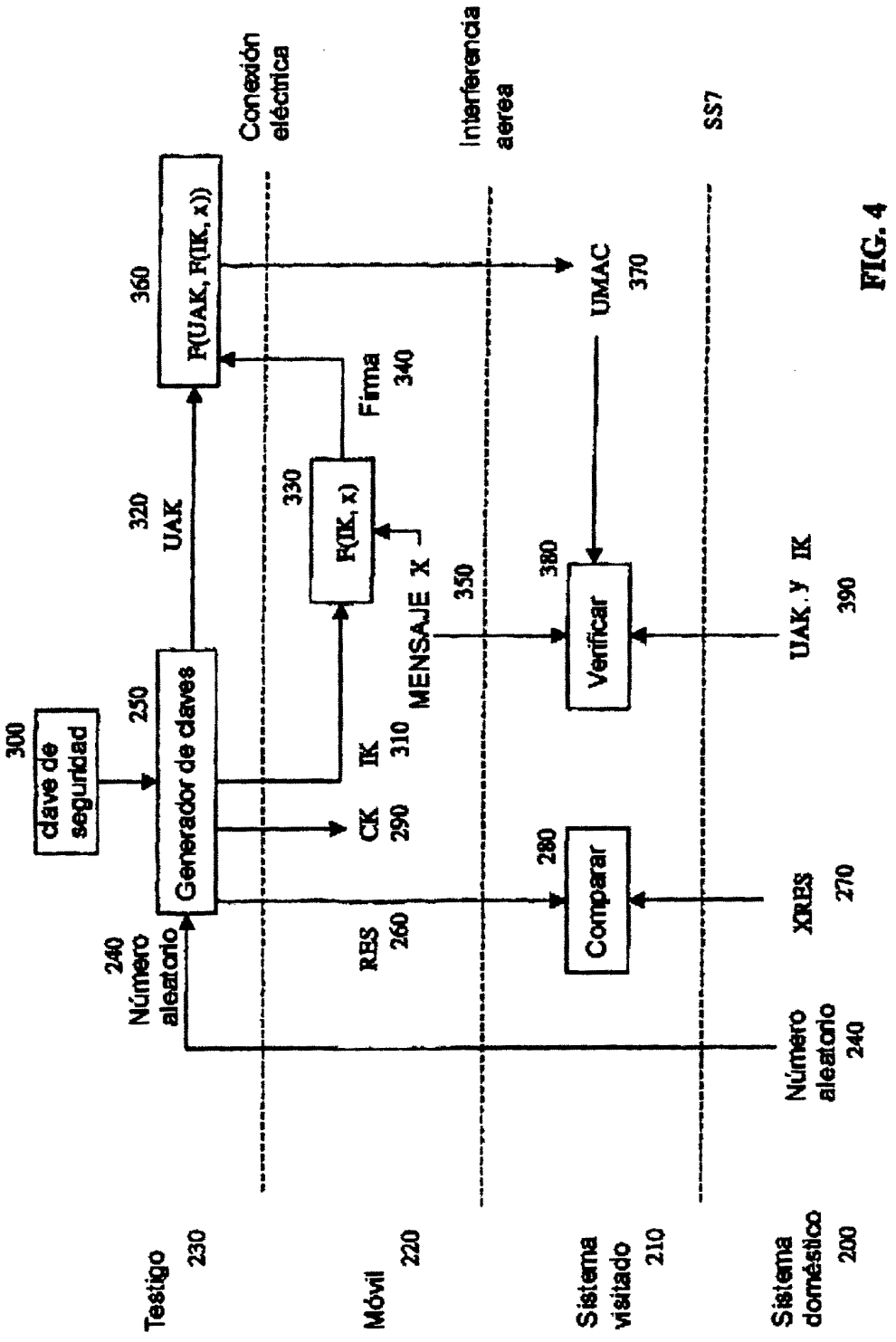
Conexión eléctrica
Interferencia aérea
SS7
360
F(UAK, F(IK, x))
UMAC
370
Fima
340
330
F(IK, x)
320
UAK
MENSAJE X
350
380
Verificar
UAK, Y IK
390
300
clave de seguridad
250
Generador de claves
CK
290
IK
310
280
Comparar
XRES
270
240
Número aleatorio
RES
260
Número aleatorio
240
Testigo
230
Móvil
220
Sistema visitado
210
Sistema doméstico
200

FIG. 4

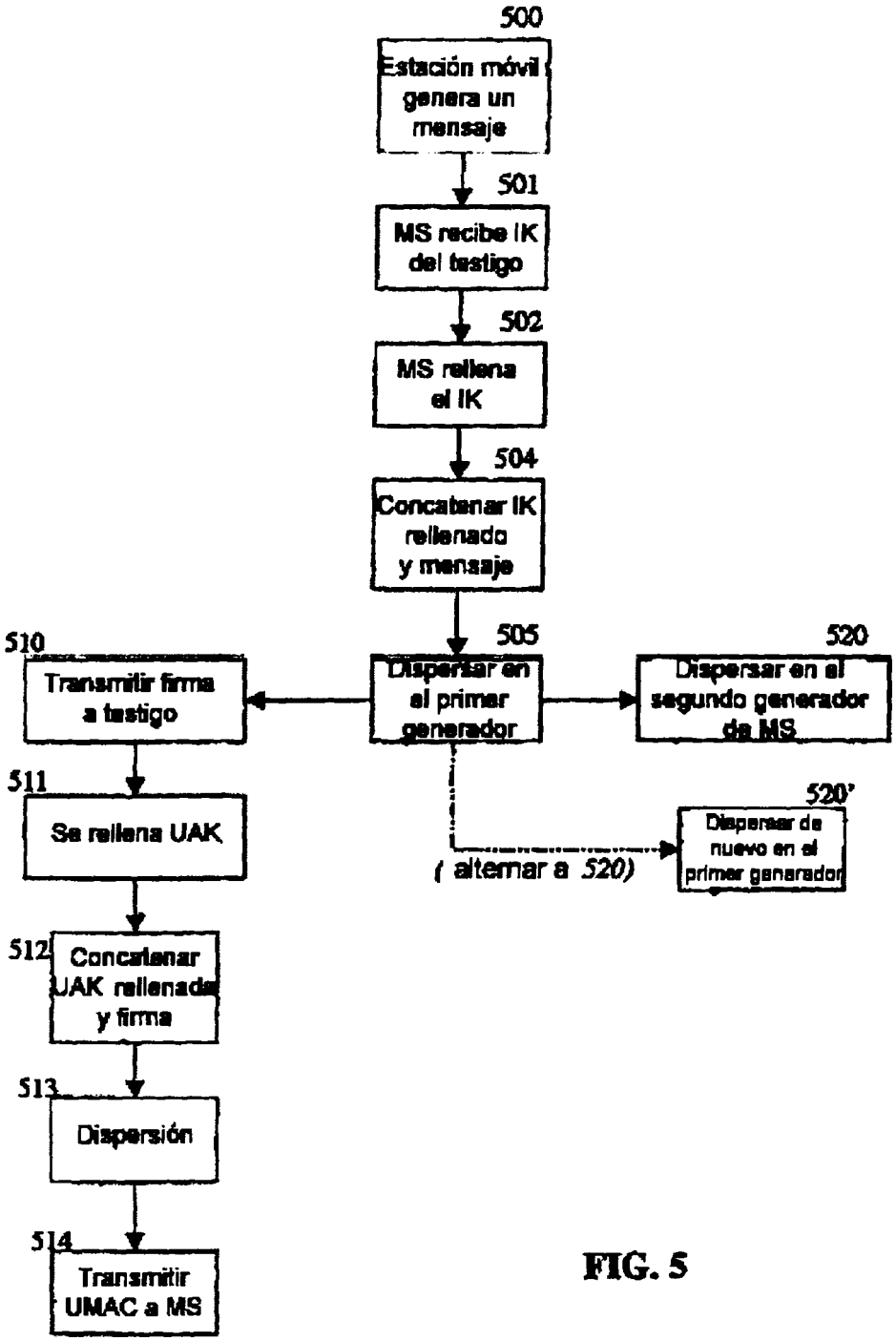
500
Estación móvil genera un mensaje
501
MS recibe IK del testigo
502
MS rellena el IK
504
Concatenar IK rellenado y mensaje
505
Dispersar en el primer generador
510
Transmitir firma a testigo
520
Dispersar en el segundo generador de MS
511
Se rellena UAK
520'
Dispersar de nuevo en el primer generador
(alternar a 520)
512
Concatenar UAK rellenada y firma
513
Dispersión
514
Transmitir UMAC a MS

FIG. 5