(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 364 574**

(51) Int. Cl.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06720264 .8**
(96) Fecha de presentación : **03.02.2006**
(97) Número de publicación de la solicitud: **1854263**
(97) Fecha de publicación de la solicitud: **14.11.2007**

(54) Título: **Secuencia inicial segura para comunicaciones inalámbricas.**

(30) Prioridad: **04.02.2005 US 650358 P**
18.02.2005 US 654133 P

(45) Fecha de publicación de la mención BOPI:
07.09.2011

(45) Fecha de la publicación del folleto de la patente:
07.09.2011

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

(72) Inventor/es: **Rose, Gregory Gordon;**
Semple, James y
Nasielski, John Wallace

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

DESCRIPCIÓN

Secuencia Inicial segura para comunicaciones inalámbricas

Antecedentes

Campo

La presente invención se refiere en general a sistemas y procedimientos para asegurar las comunicaciones inalámbricas. Más específicamente, una característica de la invención proporciona un esquema novedoso de autenticación y conformidad de claves para dispositivos que soportan mecanismos de autenticación de red heredados, para proporcionar claves de seguridad de la aplicación aprovechando la autenticación inalámbrica heredada y los mecanismos de conformidad de clases.

Antecedentes

Un tipo de tecnología celular para las comunicaciones inalámbricas se define mediante el protocolo del Sistema Global para Móviles (GSM), que funciona en redes de telefonía inalámbrica de la segunda generación (2G). El GSM se extiende además mediante redes más nuevas, tal como el Servicio de Paquetes de Radio General (GPRS), también conocidas como redes 2.5G, que ofrecen contenido de Internet y servicios de datos basados en paquetes para redes GSM. El GSM y el GPRS se usan para muchos tipos de comunicaciones inalámbricas que incluyen datos de voz, navegación por Internet, e-mail y multimedia. El GSM incorpora varios mecanismos de seguridad para proteger el contenido comunicado a través de tales sistemas. Los proveedores de servicios y asimismo los usuarios confían en estos mecanismos de seguridad para la privacidad de sus comunicaciones y la protección de sus datos y los proveedores de servicios usan estas medidas de seguridad para autenticar a sus abonados con finalidades de facturación. Estos mecanismos de seguridad funcionan típicamente mediante la autenticación de los terminales móviles del usuario en la red y pudiendo cifrar las transmisiones posteriores. Sin embargo, las medidas de seguridad GSM son vulnerables al ataque por terceras partes, debido a la debilidad de los protocolos de seguridad GSM, tal como ataques de estaciones base falsas que surgen de una carencia de autenticación de red, la posibilidad de repetición de los protocolos de seguridad y la debilidad en los algoritmos de cifrado GSM.

Estas debilidades de seguridad se acometieron en el desarrollo de los protocolos de seguridad de las normas de comunicación inalámbrica de la tercera generación (3G). En particular el protocolo de Autenticación y Conformidad de Claves (AKA) desarrollado para el Sistema Universal de Telecomunicaciones Móviles (UMTS) incluye características tales como un número de secuencia y un Código de Autenticación de Mensajes (MAC) que impiden los ataques de estaciones base falsas a las que es susceptible el GSM. Por ello los abonados de móviles que usan un módulo de identidad de servicio de usuario UMTS (USIM) para autenticación de la red no son vulnerables a los ataques planteados contra usuarios de un módulo de identidad de abonado GSM (SIM).

Las entidades de normalización 3G están desarrollando también una Arquitectura de Autenticación Genérica (GAA), por ejemplo, en el documento del proyecto de asociación para la tercera generación 3GPP 33.220 Arquitectura de Autenticación Genérica (GAA), para una arquitectura de la secuencia inicial genérica. Esta arquitectura descansa en el protocolo AKA 3G para establecer claves entre un equipo de usuario (UE) de un abonado móvil y una nueva entidad de servidor conocida como Función de Servidor de Secuencia Inicial (BSF). A partir de estas claves se pueden deducir y proporcionar por la BSF claves adicionales a varias Funciones de Aplicación de Red (NAF), como una forma de establecer las claves de seguridad compartidas entre las NAF y el UE apropiado.

Las técnicas bajo desarrollo descansan en la autenticación 3G y en los procedimientos de conformidad de claves, tal como los soportados en un Módulo de Identidad de Abonado Universal UMTS (USIM), con sus mejoras de seguridad inherentes comparadas con 2G o sistemas heredados anteriores tal como el GSM. Por ejemplo, la Arquitectura de Autenticación Genérica (GAA) y la Arquitectura de Secuencia Inicial Genérica (GBA) se especifican para las redes 3G y se construyen sobre la infraestructura de seguridad de las redes móviles 3G (es decir, la seguridad basada en USIM) para proporcionar una autenticación mutua segura entre el equipo de usuario móvil y el servidor de red que facilite las aplicaciones y/o servicios de red.

Sin embargo, estas técnicas de autenticación mutua (por ejemplo, GAA y GBA) no están disponibles para sistemas de comunicaciones desarrollados anteriormente (por ejemplo, 2G), tal como los protocolos de autenticación y conformidad de claves (AKA) de GSM, por ejemplo. Estos protocolos GSM son susceptibles ante ataques por repetición de modo que un atacante puede forzar la reutilización de claves y posiblemente explotar las debilidades en algunos contextos para revelar las claves y con ello debilitar la seguridad. Por ello, se necesita un procedimiento para claves de seguridad para la aplicación de secuencia inicial a partir de la autenticación y conformidad de claves GSM de tal manera que no sea susceptible a ataques por repetición y las claves no se puedan revelar fácilmente.

Por ello, hay una necesidad de establecer técnicas mediante las que se pueda extender la Arquitectura de Autenticación Genérica (GAA), especificada para redes 3G, para dar soporte a sistemas heredados (por ejemplo, sistemas 2G o anteriores). Esto permitiría a los abonados con dispositivos GSM u otros, que tengan Módulos de Identidad de Abonado (SIM), ser provistos con claves para su uso en aplicaciones de redes móviles y/o servicios sin que necesiten la sustitución de sus SIM por las USIM de UMTS. Más aún, tal procedimiento no debería introducir

debilidades en la arquitectura de autenticación genérica debidas a las vulnerabilidades de la autenticación GSM en sí.

El documento US 2004/0015692 describe un procedimiento de autenticación en una red de comunicaciones móviles que comprende el medio de autenticación de abonado en una entidad de red y la autenticación de la entidad de red respecto al medio de identificación del abonado.

Sumario

De acuerdo con la invención se proporciona el procedimiento de la reivindicación 1.

De acuerdo con la invención se proporciona también el terminal móvil de la reivindicación 12.

De acuerdo con la invención se proporciona también el medio que pueda leer una máquina de la reivindicación 29.

De acuerdo con la invención se proporciona también el producto de software de la reivindicación 30.

Se describe un procedimiento de autenticación mutua para acordar con seguridad las claves de seguridad de la aplicación con terminales móviles que soporten módulos de identidad de abonado heredados (por ejemplo, SIM de GSM y R-UIM de CDMA2000, que no soporten mecanismos AKA de 3G). Se implementa un intercambio de claves interpelación-respuesta entre la función del servidor de secuencia inicial (BSF) y el terminal móvil (MT). La BSF recibe unos parámetros de autenticación de la red del Registrador de Localización Local (HLR) que corresponden a este terminal móvil (por ejemplo RAND de GSM, SRES, Kc) y genera una interpelación de autenticación que involucra al RAND y la envía al MT bajo el mecanismo de clave pública autenticada por el servidor. Esta interpelación de autenticación puede incluir parámetros adicionales tal como un número aleatorio, información de identidad, marcados de tiempo, números de secuencia y claves públicas de Diffie-Hellman.

El MT recibe la interpelación de autenticación y determina si se ha originado desde la BSF en base a un certificado del servidor de la secuencia inicial. El MT había formulado una respuesta a la interpelación de autenticación en base a las claves deducidas de la interpelación de autenticación (por ejemplo, un número aleatorio) y a una clave secreta precompartida (por ejemplo, en el SIM de GSM). Esto es, el SIM en el MT puede deducir claves secretas (por ejemplo SRES y Kc) usadas por la función de servidor de secuencia inicial en base al número aleatorio RAND recibido en la interpelación de autenticación y a la clave secreta precompartida almacenada en el SIM. La respuesta de autenticación puede incluir parámetros adicionales tales como una información de identidad de número aleatorio cifrado, marcados de tiempo, números de secuencia y claves públicas de Diffie-Hellman. La BSF recibe la respuesta de autenticación y determina si se originó desde el MT. El mecanismo de respuesta a la interpelación hace uso de los mecanismos de clave pública para verificar el origen de la interpelación y las claves secretas precompartidas para verificar el origen de la respuesta. Por ejemplo, la BSF puede recalcular independientemente uno o más parámetros en la respuesta de autenticación (por ejemplo usando o en base al RAND, SRES y/o Kc que obtuvo desde el HLR) para verificar que uno o más parámetros recibidos en la respuesta de autenticación son los mismos.

En el caso en que estos mensajes se hayan autenticado, la BSF y el MT pueden calcular entonces las claves de seguridad de la aplicación en base al RAND, SRES, Kc y/o parámetros adicionales que se pueden haber transmitido entre la BSF y el MT. Nótese que las claves SRES y Kc son conocidas independientemente por la BSF y el MT y no se transmiten entre ellos. Las claves de seguridad de la aplicación se pueden enviar desde la función del servidor de secuencia inicial a la función de aplicación de red solicitante de modo que el terminal móvil y la función de aplicación de red compartan las claves de seguridad de la aplicación y puedan usarlas para asegurar la comunicación entre ellos.

Se describe un procedimiento para la autenticación de un terminal móvil heredado para comunicarse con una función de aplicación de red, que comprende: (a) la generación de una interpelación de autenticación en una función de servidor de secuencia inicial, (b) el envío de la interpelación de autenticación al terminal móvil, en el que el terminal móvil pueda verificar el origen de la interpelación de autenticación en base al certificado de servidor de secuencia inicial obtenido previamente asociado con la Función de Servidor de Secuencia Inicial, (c) la recepción de una respuesta de autenticación en la función de servidor de secuencia inicial que incluye un primer parámetro calculado con una primera clave generada en el terminal móvil, (d) la verificación de si la respuesta de autenticación se originó desde el terminal móvil mediante el recálculo del primer parámetro en la función de servidor de secuencia inicial sobre una segunda clave proporcionada a la función de servidor de secuencia inicial y (e) la comparación de los primeros parámetros recibidos en la respuesta de autenticación con el primer parámetro recalculado por la función de servidor de secuencia inicial. Se considera que la respuesta de autenticación se ha originado en el terminal móvil si ambos primeros parámetros son el mismo.

La primera clave se puede obtener desde un módulo de identificación de abonado, que puede ser un Módulo de Identidad de Abonado (SIM) del Sistema Global para Móviles (GSM) o un Módulo de Autenticación de CDMA2000, almacenado en el terminal móvil. La segunda clave se puede obtener desde un registrador de localización local conectado comunicativamente con la función de servidor de secuencia inicial, la primera y segunda claves se pueden generar en base a los mismos algoritmos de seguridad y a una clave secreta precompartida conocida para un módulo de identificación de abonado en el terminal móvil y una base de datos de red conectada

comunicativamente a la función de servidor de secuencia inicial. La interpelación de autenticación puede incluir un número aleatorio como un parámetro y el número aleatorio y la clave secreta precompartida, almacenada en un módulo de identificación de abonado en el terminal móvil, se usan por el módulo de identificación de abonado para generar la primera clave usada para calcular el primer parámetro en la respuesta de autenticación. La segunda clave proporcionada a la función de servidor de secuencia inicial se puede generar en base a una copia de la clave secreta precompartida almacenada fuera del terminal móvil y al número aleatorio en la interpelación de autenticación. El primer parámetro de la respuesta de autenticación puede incluir un código de autenticación de mensaje calculado con la primera clave y usado por la función de servidor de secuencia inicial para verificar el origen de la respuesta de autenticación.

En algunas implementaciones, se puede generar una tercera clave en la función de servidor de secuencia inicial en base a la segunda clave; el primer parámetro se recalcula en la función de servidor de secuencia inicial usando la tercera clave.

Adicionalmente, el procedimiento descrito puede incluir adicionalmente (a) el cálculo de una cuarta clave en la función de servidor de secuencia inicial en base a la segunda clave, que se calcula también independientemente por el terminal móvil usando la primera clave y (b) el envío de la cuarta clave desde la función de servidor de secuencia inicial a una función de aplicación de red solicitante de modo que el terminal móvil y la función de aplicación de red compartan la cuarta clave para la seguridad de las comunicaciones entre ellos.

Otra característica descrita proporciona un dispositivo de red que comprende: (a) una interfaz de comunicaciones para comunicar con terminales móviles inalámbricos y (b) un circuito de procesamiento conectado a la interfaz de comunicaciones y configurado para implementar una función de servidor de secuencia inicial para autenticar al terminal móvil. El circuito de procesamiento puede autenticar el terminal móvil mediante (a) la generación de la interpelación de autenticación que incluye un número aleatorio, (b) el envío de la interpelación de autenticación al terminal móvil, en el que el terminal móvil puede verificar el origen de la interpelación de autenticación en base a un certificado del servidor de secuencia inicial previamente obtenido asociado con la función del servidor de secuencia inicial, (c) la recepción de una respuesta de autenticación desde el terminal móvil, incluyendo la respuesta de autenticación un primer parámetro calculado con una primera clave en base al número aleatorio, una clave secreta precompartida y un algoritmo, en el que la clave secreta precompartida y el algoritmo son conocidos para un módulo de identificación de abonado en el terminal móvil y para una base de datos de red conectada comunicativamente con la función de servidor de secuencia inicial, (d) el cálculo de un segundo parámetro en la función de servidor de secuencia inicial en base a una segunda clave proporcionada al servidor de secuencia inicial por la base de datos de red y (e) la comparación del primer parámetro y el segundo parámetro, en el que la respuesta de autenticación se considera que se ha originado desde el terminal móvil si el primer y el segundo parámetros son el mismo. En algunas implementaciones, el módulo de identificación de abonado puede ser uno de o bien un Módulo de Identidad de Abonado (SIM) del Sistema Global para Móviles (GSM) o un Módulo de Autenticación de CDMA2000. Adicionalmente, el circuito de procesamiento se puede configurar además para implementar la función de servidor de secuencia inicial para autenticar al terminal móvil mediante (a) el cálculo de una cuarta clave en la función de servidor de secuencia inicial en base a la segunda clave, que se calcula también en el terminal móvil en base a la primera clave y (b) el envío de la cuarta clave desde la función de servidor de secuencia inicial a una función de aplicación de red solicitante de modo que el terminal móvil y la función de aplicación de red compartan la cuarta clave. El circuito de procesamiento se puede configurar además para implementar la función de servidor de secuencia inicial para autenticar el terminal móvil comparando el primer parámetro recibido en la respuesta de autenticación con el primer parámetro calculado por la función de servidor de secuencia inicial, en el que la respuesta de autenticación se considera que se ha originado desde el terminal móvil si ambos primeros parámetros son el mismo.

Otro procedimiento más descrito es para la autenticación de un terminal móvil heredado para comunicar con una función de aplicación de red, que comprende: (a) la recepción de la interpelación de autenticación en el terminal móvil que incluye un número aleatorio, (b) la verificación de si la interpelación de autenticación se origina en una función de servidor de secuencia inicial en base a un certificado de servidor de secuencia inicial obtenido previamente asociado con la función de servidor de secuencia inicial, (c) la generación de una respuesta de autenticación en base a una primera clave generada por un módulo de identificación de abonado heredado en el terminal móvil y (d) proporcionar la primera clave desde el módulo de identificación de abonado en el terminal móvil en respuesta a la recepción del número aleatorio recibido en la interpelación de autenticación. El procedimiento puede incluir además la generación de la primera clave en el módulo de identificación de abonado que usa un número aleatorio, una clave secreta precompartida y un algoritmo. La clave secreta precompartida y el algoritmo se almacenan ambos en el módulo de identificación de abonado y en una base de datos de red conectada comunicativamente a la función de servidor de secuencia inicial. En algunas implementaciones, se puede generar la primera clave usando parámetros adicionales transmitidos en la interpelación de autenticación y en la respuesta.

El procedimiento puede incluir además el cálculo de una tercera clave en el terminal móvil en base a la primera clave. La tercera clave puede calcularse también independientemente en la función de servidor de secuencia inicial en base a una segunda clave proporcionada a la función de servidor de secuencia inicial por la base de datos de red. La tercera clave se envía desde la función de servidor de secuencia inicial a una función de aplicación de redes solicitante de modo que el terminal móvil y la función de aplicación de red compartan la tercera clave.

Otra característica descrita proporciona un terminal móvil que comprende: (a) una interfaz de comunicaciones inalámbrica para comunicar con una función de servidor de secuencia inicial, (b) un módulo de identificación de abonado para almacenamiento de una clave secreta precompartida y un algoritmo y (c) un circuito de procesamiento configurado para funcionar con un protocolo de comunicación heredado y autenticar el terminal móvil en un protocolo de interpelación-respuesta con una función de servidor de secuencia inicial. El circuito de procesamiento puede funcionar mediante (a) la recepción de la interpelación de autenticación, que incluye un número aleatorio, desde una función de servidor de secuencia inicial, (b) la determinación de si la interpelación de autenticación se originó desde la función de servidor de secuencia inicial en base a un certificado de servidor de secuencia inicial previamente obtenido asociado con la función de servidor de secuencia inicial y (c) la generación de una respuesta de autenticación que incluye un primer parámetro calculado con una primera clave, en la que la primera clave se genera a partir del número aleatorio, la clave secreta precompartida y el algoritmo. Adicionalmente, el circuito de procesamiento puede (a) generar una tercera clave deducida en base a la primera clave y otros parámetros transmitidos en la interpelación y respuesta de autenticación y (b) generar un código de autenticación de mensajes calculado usando la tercera clave. El código de autenticación del mensaje puede estar incluido en la respuesta de autenticación al servidor de secuencia inicial. El módulo de identificación de abonado puede generar la primera clave en base al número aleatorio, la clave secreta precompartida y el algoritmo.

El módulo de identificación de abonado puede ser un Módulo de Identidad de Abonado (SIM) de acuerdo con el protocolo del Sistema Global para Móviles (GSM). La clave secreta precompartida se puede emplear también para permitir al terminal móvil establecer comunicaciones a través de una red inalámbrica heredada.

Breve descripción de los dibujos

La Figura 1 es un diagrama de bloques que ilustra un sistema de comunicación en el que un servidor de secuencia inicial y un terminal móvil heredado se pueden autenticar mutuamente entre sí de acuerdo con una implementación.

La Figura 2 es un diagrama de bloques que ilustra un terminal móvil configurado para realizar la autenticación mutua con la función de servidor de secuencia inicial operativa en una red de comunicación de acuerdo con una implementación.

La Figura 3 es un diagrama de bloques que ilustra un dispositivo de red configurado para realizar una función de servidor de secuencia inicial para autenticar una estación móvil de acuerdo con una implementación.

La Figura 4 ilustra un procedimiento de realización de un mecanismo de interpelación-respuesta que autentica mutuamente un terminal móvil heredado y una función de servidor de secuencia inicial de acuerdo con una implementación.

La Figura 5 ilustra un procedimiento general de autenticación de un terminal móvil usando una función de servidor de secuencia inicial y la autenticación de la función de servidor de acuerdo con una implementación.

La Figura 6 ilustra un procedimiento de realización de un protocolo de interpelación-respuesta entre un terminal móvil de acuerdo con GSM y una función de servidor de secuencia inicial para autenticarse de modo seguro entre ellos para funciones de aplicación de red de acuerdo con una implementación.

La figura 7 ilustra un procedimiento alternativo de realización de un protocolo des interpelación-respuesta entre un terminal móvil de acuerdo con GSM y una función de servidor de secuencia inicial para autenticarse con seguridad entre sí para funciones de aplicación de red de acuerdo con una implementación.

Descripción detallada

En la descripción a continuación, se dan detalles específicos para proporcionar una comprensión global de las realizaciones. Sin embargo, se comprenderá por un experto la técnica que se pueden poner en práctica las realizaciones sin estos detalles específicos. Por ejemplo, los circuitos se pueden mostrar en diagramas de bloques para no ofuscar las realizaciones con detalles innecesarios. En otros casos, pueden no mostrarse circuitos estructuras y técnicas bien conocidas en detalle para no ofuscar las realizaciones.

También, se hace notar que las realizaciones se pueden describir como un proceso que se representa como un gráfico de flujo, un diagrama de flujo, un diagrama de estructura o un diagrama de bloques. Aunque en un gráfico de flujo se pueden describir las operaciones como un proceso secuencial, muchas de las operaciones se pueden realizar en paralelo o concurrentemente. Además, se puede redisponer el orden de las operaciones. Un proceso se termina cuando sus operaciones se han completado. Un proceso puede corresponder a un procedimiento, una función, a una rutina, una subrutina, o un subprograma, etc. Cuando un proceso se corresponde con una función, su finalización corresponde a una devolución desde la función a la función de llamada o a la función principal.

Más aún, un medio de almacenamiento puede representar uno o más dispositivos para almacenar los datos, incluyendo memoria sólo de lectura (ROM), memoria de acceso aleatorio (RAM), medios de almacenamiento en discos magnéticos, medios de almacenamiento óptico, dispositivos de memoria flash y/u otros medios que pueda leer una máquina para el almacenamiento de información. La expresión “medio que pueda leer una máquina”

incluye, pero sin limitarse a, dispositivos de almacenamiento fijos y extraíbles, dispositivos de almacenamiento ópticos, canales inalámbricos y diversos otros medios capaces de almacenar, contener o portar instrucciones y/o datos.

Adicionalmente, las realizaciones se pueden implementar mediante hardware, software, firmware, middleware, micro códigos o una combinación de los mismos. Cuando se implementa en software, firmware, middleware o micro códigos, el código de programa o segmentos de código para realizar las tareas necesarias se puede almacenar en un medio que pueda leer una máquina tal como un medio de almacenamiento u otros almacenamientos. Un procesador puede realizar las tareas necesarias. Un segmento de código puede representar un procedimiento, una función, un subprograma, un programa, una rutina, una subrutina, un módulo, un paquete de software, una clase o una combinación de instrucciones, estructuras de datos o sentencias de programa. Un segmento de código se puede conectar a otro segmento de código o circuito de hardware mediante el paso y/o recepción de información, datos, argumentos, parámetros o contenido de memoria. La información, argumentos, parámetros, datos, etc. se puede pasar, enviar o transmitir a través de un medio adecuado que incluye compartir la memoria, el paso de mensajes, el paso de testigos, transmisión por red, etcétera.

En la siguiente descripción, cierta terminología se usa para describir ciertas características de una o más realizaciones de la invención. Por ejemplo las expresiones “terminal móvil”, “equipo de usuario”, “dispositivo móvil”, “dispositivo inalámbrico” y “dispositivo móvil inalámbrico” se usan de modo intercambiable para referirse a teléfonos móviles, dispositivos de busca, modems inalámbricos, asistentes digitales personales, gestores de información personal (PIM), miniordenadores portátiles, ordenadores portátiles y/u otros dispositivos de comunicación/cálculo móviles que se comuniquen, al menos parcialmente, a través de la red celular. El término “heredado” se usa para referirse a redes, protocolos y/o dispositivos móviles que son previos a la 3G, funcionan con un protocolo previo a la 3G o que emplean una SIM que cumple con GSM o un Módulo de Autenticación que cumple con CDMA o Módulo de Autenticación MN-AAA. Adicionalmente, el término módulo de identificación de abonado se usa para referirse a un Módulo de Identidad de Abonado (SIM) que cumple con GSM, un Módulo de Autenticación que cumple con CDMA o Módulo de Autenticación MN-AAA o cualquier otro módulo incluido típicamente en un terminal móvil para identificar al terminal móvil en una red inalámbrica.

Una característica proporciona una forma de extender la Arquitectura de Autenticación Genérica para soportar sistemas heredados, de modo que los abonados que mantienen un módulo de identidad de abonado (SIM) de GSM puedan estar provistos con claves para su uso en aplicaciones móviles sin necesitar la sustitución de la SIM por un módulo de identidad de servicio de usuario que cumpla con 3G, UMTS (USIM).

La Figura 1 es un diagrama de bloques que ilustra un sistema de comunicación en el que se pueden autenticar mutuamente entre sí un servidor de secuencia inicial y un terminal móvil heredado de acuerdo con una implementación. Una arquitectura de red 100, tal como un sistema de comunicación de acuerdo con GSM o de acuerdo con CDMA2000, incluye un terminal móvil (MT) 102, un registro de localización local (HLR) 104, una función de servidor de secuencia inicial (BSF) 106 y al menos una función de aplicación de red (NAF) 108. El HLR 104 y la BSF 106 se pueden alojar en uno o más dispositivos de red y/o servidores que sean parte de la infraestructura de la arquitectura de red 100. El HLR 104 incluye una base de datos que contiene información de abonados móviles para un proveedor inalámbrico, que incluye una identidad de abonado móvil internacional (IMSI) para cada MT 102 que pertenece al abonado. El IMSI es un número único que se asocia con un MT 102 en la red. EL IMSI se almacena también en el módulo de identidad de abonado (SIM) de cada MT 102 y se envía por el MT al HLR de red para buscar información acerca del MT 102.

El MT 102 puede ser un dispositivo de comunicación inalámbrico heredado que se registra o conecta con un proveedor usando un protocolo predefinido (por ejemplo un protocolo previo a 3G) para comunicarse a través de la red 100. En algunas implementaciones, este proceso de registro con un proveedor de servicios puede involucrar la autenticación del MT 102 mediante el uso de la clave secreta precompartida (por ejemplo, almacenada en un SIM de GSM, un Módulo de Autenticación de CDMA u otro módulo heredado). Por ejemplo, el MT 102 puede contener una SIM de acuerdo con GSM o un Módulo de Autenticación de acuerdo con CDMA2000 para permitir al MT 102 operar en las redes GSM o CDMA2000 y permitirle ser autenticado por la red para comunicaciones a través del aire.

Una vez el MT 102 es autenticado por el proveedor de servicios para comunicaciones a través de la red, un aspecto de la invención añade otra capa de autenticación para permitir aplicaciones de redes seguras. Este mecanismo de autenticación adicional es dependiente del operador de la red subyacente o del mecanismo de autenticación del operador. La capa adicional de autenticación usa las claves existentes, en el SIM o módulo de autenticación, junto con un protocolo novedoso para establecer claves que sean independientes de la red o servicios de seguridad del portador. Este nuevo mecanismo de autenticación proporciona claves para autenticación, otras finalidades, compartidas entre el MT 102 y una NAF 108 específica, distribuida a las NAF por medio de la BSF 106. La NAF 108 puede ser una aplicación que opere en un dispositivo de red, tal como unas aplicaciones de transacciones comerciales y/o servicios basados en la localización, por ejemplo.

Cuando el MT 102 está listo para comenzar el uso de una aplicación de red, inicia el contacto con la NAF 108 a través de un enlace de comunicaciones 110. Si el MT y la NAF no comparten ya las claves apropiadas, entonces el NAF 108 realiza una solicitud de claves de autenticación a través de una interfaz 112, a la BSF 106. Si no lo ha

realizado ya, el MT 102 y la BSF 106 acuerdan las claves con el MT 102 a través de un enlace de autenticación 114.

Se puede emplear un intercambio de claves de Diffie-Hellman como parte del proceso del acuerdo de claves entre el MT 102 y la BSF 106. El intercambio de claves de Diffie-Hellman es un protocolo criptográfico que permite a dos partes que no tengan previo conocimiento mutuo establecer conjuntamente una clave secreta compartida a través de un canal de comunicaciones inseguro. En una aplicación, esta clave secreta compartida se puede usar a continuación para cifrar las comunicaciones posteriores usando un codificador de clave simétrica.

Sin embargo, sin más, los algoritmos de intercambio de claves de Diffie-Hellman son susceptibles a ataques por "persona interpuesta" que minan la seguridad de este algoritmo. Esto es de particular preocupación cuando se intercambia información a través de un medio inalámbrico para realizar transacciones comerciales y/o confidenciales entre un MT 102 y una NAF 108.

Una característica de la invención proporciona un protocolo que permite a la BSF 106 y al MT 102 acordar una clave secreta pública o compartida en una forma que no sea susceptible a las debilidades inherentes al GSM y/o CDMA2000. En particular, el MT 102 está provisto primero con un certificado digital para autenticar a la BSF 106. Esto permite a las comunicaciones desde la BSF 106 hacia el MT 102 estar firmadas digitalmente o portadas en un canal de servidor autenticado, permitiendo así al MT 102 asegurarse de que las claves o parámetros recibidos durante el proceso de autenticación llegan desde la BSF 106 y no desde otra entidad que intente un ataque por "persona interpuesta" o repetición. Por ello, el procedimiento presente se puede aplicar para extender el esquema de autenticación de la arquitectura de secuencia inicial genérica 3G a protocolos, distintos del AKA UMTS, que no se benefician por sí mismos de la autenticación de red.

La Figura 2 es un diagrama de bloques que ilustra un terminal móvil (MT) 200 configurado para realizar una autenticación mutua con la función de servidor de secuencia inicial operativa en una red de comunicación. El MT 200 incluye un circuito de procesamiento 202 (por ejemplo un procesador) conectado a la interfaz de comunicaciones 202 para comunicar con una red inalámbrica, y una tarjeta del Módulo de Identidad de Abonado (SIM) 204. El circuito de procesamiento 202 se puede configurar para realizar parte o la totalidad de los procedimientos ilustrados en las Figuras 4, 5, 6 y 7. El SIM 204 puede contener una clave secreta Ki, una implementación de la autenticación GSM y algoritmos de conformidad de clave (es decir, algoritmos A3/A8 de GSM) y se inserta en un MT 102 que contiene una clave pública o certificado de servidor digital de una clave pública que corresponde a una clave privada en la BSF 106. En particular el SIM 204 puede ser una tarjeta inteligente heredada estándar configurada para su uso en una red GSM. La clave pública o certificado de servidor puede corresponder a una clave pública RSA o a otras técnicas de clave pública que permiten que se use también la firma digital, por ejemplo, DSA (algoritmo de firma digital). La BSF 106 y el MT 102 pueden compartir también un generador predeterminado P o un grupo cíclico, tal como el subgrupo multiplicativo de un campo finito o un punto en una curva elíptica, permitiéndoles emplear el intercambio de claves de Diffie-Hellman. En realizaciones alternativas, el MT 200 puede incluir un módulo de autenticación de acuerdo con CDMA2000 en lugar del SIM 204.

La Figura 3 es un diagrama de bloques que ilustra un dispositivo de red configurado para realizar una función de servidor de secuencia inicial (BSF) para la autenticación de una estación móvil (MT) de acuerdo con un aspecto de la invención. El dispositivo de red 300 incluye un circuito de procesamiento 302 (por ejemplo un procesador) conectado a una interfaz de comunicaciones 306 para comunicar con la red inalámbrica y un dispositivo de memoria 304. El circuito de procesamiento 302 se puede configurar para ejecutar la función de servidor de secuencia inicial mientras mantiene las claves y/o parámetros para implementar el intercambio de claves de Diffie-Hellman con un MT. Por ejemplo, el circuito de procesamiento 302 se puede configurar para realizar parte o la totalidad de los procedimientos ilustrados en las Figuras 4, 5, 6 y 7.

La Figura 4 ilustra un procedimiento de realización de un mecanismo de interpelación-respuesta que autentica mutuamente un terminal móvil, que tenga una SIM heredada, y una función de servidor de secuencia inicial de acuerdo con una implementación. Este mecanismo de interpelación-respuesta hace uso de mecanismos de clave pública para verificar el origen de la interpelación y de claves secretas precompartidas para verificar el origen de la respuesta.

La función de servidor de secuencia inicial (BSF) genera una interpelación de autenticación y la envía al terminal móvil (MT) bajo un mecanismo de clave pública autenticada por el servidor 402. La interpelación de autenticación puede incluir un número aleatorio (por ejemplo, RAND) que se deduce de una clave secreta precompartida (por ejemplo, Ki) conocida en una base de datos de red y un módulo de identificación de abonado en el MT. Por ejemplo, la clave secreta precompartida Ki y el número aleatorio (por ejemplo RAND) se pueden usar para generar claves secretas (por ejemplo SRES y Kc) que se usan para generar los parámetros de interpelación de autenticación. La interpelación de autenticación puede incluir también parámetros adicionales, tales como marcados de tiempos, otros números aleatorios, información de identidad, claves públicas de Diffie-Hellman, etc. y se envía a través de un canal firmado digitalmente y/o autenticado por el servidor.

El MT recibe la interpelación de autenticación y verifica si se origina desde la BSF en base al certificado de servidor de secuencia inicial 404. Tal certificado de servidor de secuencia inicial (por ejemplo una clave pública) se puede haber proporcionado al MT y a la BSF en los ajustes, fuera de línea y/o durante un proceso previo. El MT formula

una respuesta a la interpelación de autenticación en base a las claves deducidas y/o proporcionadas por el módulo de identificación de abonado en el MT 406. Estas claves secretas se pueden generar por el módulo de identificación de abonado en base al número aleatorio recibido en la interpelación de autenticación y la clave secreta precompartida almacenada en el módulo de identificación de abonado. Por ejemplo, el número aleatorio (por ejemplo RAND) recibido en la interpelación de autenticación y la clave secreta precompartida (por ejemplo Ki), almacenada en el módulo de identificación de abonado del MT, se pueden usar para generar claves (por ejemplo SRES y Kc) que se usan para generar los parámetros de respuesta de la autenticación. Adicionalmente, en algunas implementaciones, el MT puede usar también parámetros adicionales (por ejemplo, marcado de tiempos, otros números aleatorios, información de identidad, una clave pública de Diffie-Hellman) para calcular las claves usadas para formular la respuesta de la autenticación.

La BSF recibe la respuesta de autenticación y verifica si se origina desde el MT en base a las claves secretas (por ejemplo SRES y Kc) obtenidas independientemente por la función de servidor de secuencia inicial 408. Por ejemplo, la BSF puede usar las claves secretas (por ejemplo, SRES y Kc) generadas por la base de datos de red en base al número aleatorio RAND y a la clave secreta precompartida (por ejemplo Ki). Así, un certificado de servidor de secuencia inicial se usa por el MT para verificar el origen de la interpelación mientras que las claves (por ejemplo SRES y Kc) se usan por la BSF para verificar el origen de la respuesta. Esto asegura que no tiene lugar ningún ataque por terceras partes.

A partir de la verificación y cálculos de claves independientes (por ejemplo, SRES y Kc), el MT y la BSF pueden calcular una clave compartida. Una clave de aplicación se puede generar en el terminal móvil y el servidor de secuencia inicial y el servidor de secuencia inicial se la puede proporcionar a la función de la aplicación de red solicitante para permitir las comunicaciones seguras entre el terminal móvil y la función de aplicación de red 410. Por ejemplo, la clave compartida, o una clave de aplicación deducida de la clave compartida, se puede enviar por la BSF a la función de aplicación de red (NAF) solicitante de modo que la NAF y el MT compartan una clave que se puede usar para las comunicaciones seguras entre la NAF y el MT.

La Figura 5 ilustra un procedimiento de autenticación de un terminal móvil usando una función de servidor de secuencia inicial y autenticación de la función de servidor de acuerdo con una realización de la invención. Este procedimiento se puede implementar cuando una función de aplicación de red desea acordar las claves con un terminal móvil (MT) previamente al inicio de una transacción de aplicación de red. Por ejemplo, la autenticación y acuerdo de claves (AKA) en GSM se basan en un protocolo de interpelación-respuesta. Se almacenan una clave secreta Ki así como dos algoritmos A3 y A8 en un módulo de identidad de abonado (SIM) dentro del MT así como en el registrador de localización local de red (HLR)/Centro de Autenticación (AuC). El SIM se diseña contra manipulaciones y contienen datos secretos y algoritmos que no se pueden leer fácilmente por un usuario.

Se genera una petición de una clave y se envía desde el MT, que tiene un SIM heredado en el interior, a una función de servidor de secuencia inicial (BSF) 502. La BSF obtiene información de autenticación para el MT desde un HLR de red o un AuC 504. Por ejemplo el HLR/AuC selecciona un RAND de interpelación aleatorio de 128 bits que se introduce, junto con Ki, en los dos algoritmos A3 y A8 para producir una salida de 32 bits, SRES, y una salida de 64 bits, Kc, respectivamente. Se proporcionan a continuación tripletes (RAND, SRES, Kc), que corresponden al SIM del MT solicitante, a la BSF para autenticar el SIM en el interior del MT solicitante. La BSF interpela entonces al MT con un número aleatorio RAND (generado por el HLR) y otros parámetros 506.

El MT verifica si la interpelación de autenticación se originó en la BSF esperada en base al certificado de servidor de secuencia inicial 508. Por ejemplo, esta verificación se puede realizar usando una clave pública o un certificado de servidor digital de la BSF que se ha provisto en el MT. Si la interpelación de autenticación no proviene de la BSF esperado, entonces termina el proceso. En caso contrario, se formula una respuesta de autenticación a la interpelación en base a la clave secreta proporcionada por el SIM del MT 510. Por ejemplo, el MT pasa el número aleatorio RAND al SIM (en el MT) que calcula una o más claves secretas (SRES y Kc) usando la clave secreta precompartida Ki y el número aleatorio RAND con los algoritmos A3 y A8. Las claves secretas SRES y Kc se proporcionan entonces al MT para formular la respuesta de autenticación. En una implementación, las claves secretas SRES y Kc se pueden usar para calcular un código de autenticación del mensaje o deducir o cifrar uno o más parámetros, que ese envían como parte de la respuesta de autenticación.

La respuesta de autenticación se envía desde el MT a la BSF 512. La BSF verifica entonces el origen de la respuesta de autenticación en base a una clave secreta 514 obtenida independientemente. Por ejemplo, el SRES y Kc obtenidos desde el HLR (en el triplete que corresponde al número aleatorio RAND y a la clave secreta precompartida Ki) se puede usar para validar uno o más parámetros en la respuesta de autenticación desde el MT. Por ejemplo, la BSF puede calcular independientemente el código de autenticación del mensaje (u otro parámetro en la respuesta de autenticación) usando el número aleatorio RAND, SRES y/o Kc recibidos desde el HLR. Si los parámetros (por ejemplo el código de autenticación del mensaje) calculado por el MT y la BSF coinciden, entonces se verifica el origen de la respuesta de autenticación.

En una implementación alternativa, el MT puede calcular una tercera clave usando una o más claves secretas (SRES y Kc obtenidas del SIM) y otros parámetros (obtenidos de la interpelación de autenticación o respuesta o desde el SIM). Esta tercera clave se usa entonces para formular la respuesta de autenticación (por ejemplo, calcular

el código de autenticación del mensaje). La BSF puede también calcular la misma clave dado que conoce las mismas claves y/o parámetros que el MT. Por ello, la BSF puede verificar si la respuesta de autenticación se originó en el MT.

Una vez que se verifica la respuesta de autenticación, la BSF y el MT calculan independientemente una clave compartida en base a una o más claves y/o parámetros (por ejemplo SRES, Kc y/u otros parámetros) conocidos tanto para la BSF y como para el MT 516. Esta clave compartida puede ser proporcionada ante una NAF solicitante para establecer comunicaciones o transacciones seguras entre el MT y la NAF 518.

El MT autentica las transmisiones desde la BSF por medio de un mecanismo de clave pública. La BSF interpela al MT con un número aleatorio RAND y establece que está en posesión de las claves secretas correspondientes SRES y/o Kc para autenticar las transmisiones desde el MT. Por ello, la BSF y del MT se autentican mutuamente para compartir información a partir de la que se pueden deducir las claves con la finalidad de realizar la secuencia inicial.

La Figura 6 ilustra un procedimiento de realización de un protocolo de interpelación-respuesta entre un terminal móvil 608 de acuerdo con GSM y una función de servidor de secuencia inicial 604 para autenticarse entre sí con seguridad para funciones de aplicación de red de acuerdo con una implementación. El Acuerdo de Autenticación y Claves (AKA) del GSM se basa en un protocolo de interpelación-respuesta. Para una secuencia inicial basada en una SIM heredada, el HLR/AuC y el SIM realizan cálculos similares en base a la clave secreta existente Ki y a los algoritmos A3 y A8 de GSM. En el protocolo GSM, la clave secreta Ki y el algoritmo o algoritmos de autenticación A3 y A8 se almacenan en una tarjeta inteligente de un módulo de identidad de abonado (SIM) así como en el HLR 602 de la red. El SIM 608 se diseña protegido contra manipulaciones y contienen datos y algoritmos que no se pueden leer fácilmente por un usuario. Típicamente, se usan la clave secreta Ki y el algoritmo o algoritmos de autenticación A3 y A8 para establecer un servicio a través del aire con la red.

En una realización, se puede iniciar por el MT 606 una petición de claves de autenticación recuperando su identidad de abonado móvil internacional (IMSI) 600 asociada desde su SIM 608 y enviándola a una función de servidor de secuencia inicial (BSF) 604. La BSF 604 envía el IMSI 600 al HLR 602 en el que debe verificar si el IMSI 600 pertenece a un MT que está abonado a la red. El HLR 602 puede ser operado por el proveedor de servicios para el abonado cuya SIM está contenida en el MT 606. El HLR 602 selecciona, por ejemplo, una interpelación RAND aleatoria de 128 bis y junto con la clave secreta precompartida Ki, las usa como entradas para los dos algoritmos A3 y A8 para producir una salida de 32 bits SRES de respuesta firmada y una salida secreta de una clave Kc de confidencialidad de 64 bits, respectivamente. El HLR 602 proporciona entonces el triplete (RAND, SRES, Kc) a la BSF 604, que corresponde a la identidad IMSI 600 del SIM 608. La BSF 604 genera un exponente x secreto aleatorio y calcula una clave pública P^x de Diffie-Hellman, en la que P es un generador de un grupo cíclico proporcionado previamente tanto a la BSF 604 como al MT 606, tal como un grupo multiplicativo de un campo finito o el grupo aditivo de una curva elíptica. La BSF 602 envía entonces un triplete (RAND, P^x, SIG) 610 al MT 606, en el que SIG es una firma digital calculada usando la clave privada RSA de la BSF 604. El mensaje 610 se puede mejorar adicionalmente para incluir otros parámetros autenticados por el servidor tal como un identificador de transacción.

El MT 606 recibe el triplete (RAND, P^x, SIG) 610 y usa el certificado digital de la BSF 604 para verificar el SIG. El MT 606 se supone que está provisto con el certificado digital que lo capacita para autenticar datos transmitidos desde la BSF 604. Si se considera que el dato se ha originado en la BSF, el MT 606 genera un número aleatorio y calcula P^y. El MT 606 también pasa el RAND 612 al SIM 608 que devuelve un par (SRES, Kc) 614, generado en base al RAND y Ki, al MT 606. Si el SIM 608 es auténtico, entonces debería generar el mismo SRES y Kc que fue generado por el HLR 602. El MT 606 calcula entonces un código de mensaje de autenticación MAC de P^y, con las claves SRES y Kc, y envía una respuesta (P^y, MAC) 616 a la BSF de 604. Esta respuesta 616 se puede mejorar adicionalmente para incluir otros parámetros a través de los que se calcula el MAC, tal como un identificador de transacción.

La BSF de 604 recibe P^y y verifica el MAC usando la SRES y Kc que recibió en el triplete de autenticación desde el HLR 602. Si este MAC es correcto, esto verifica que el MT 606 está en posesión del SIM 608 correcto y se puede enviar un mensaje de confirmación 618 al MT 606.

En esta realización el MT 606 y la BSF 604 han realizado de ese modo un intercambio de claves de Diffie-Hellman mutuamente autenticadas y acordado una clave P^{xy} que han calculado respectivamente. Se puede calcular entonces una clave para comunicaciones adicionales, por ejemplo, como un hash de P^{xy}, posiblemente incluyendo información adicional conocida tanto para el MT como para la BSF tal como información de identidad, RAND, SRES y Kc. En el caso en que tengan lugar los cálculos de Diffie-Hellman o se almacene la clave resultante, en el MT 606 en lugar de en el SIM 608, esta clave P^{xy} y la clave acordada resultante se deberían borrar si se extrae el SIM 608 del MT o si el MT se enciende usando un SIM 608 diferente.

Nótese que este protocolo protege contra las debilidades estándar que provienen del GSM suponiendo que el MT 606 no soporte el algoritmo A5/2. El algoritmo A5/2 permite una ruptura casi instantánea en el protocolo GSM que puede debilitar el protocolo anterior. Sin embargo, el algoritmo A5/2 se ha ido retirando en la edición 6 de las especificaciones 3GPP.

Nótese adicionalmente que un intento de ataque al protocolo por persona intermedia no puede cambiar la interpelación inicial (RAND, P^x, SIG), debido al SIG, así un atacante no puede insertar su propio P^z o usar un RAND diferente. Como mucho se podría responder a estos mensajes, pero no se puede suplantar a la BSF dado que cualquier respuesta es equivalente a usar Diffie-Hellman efímeros. A la inversa, si la BSF asegura que el RAND usado es nuevo, desde un uso de su protocolo al siguiente y asegura que la respuesta (P^y, MAC) se recibe en un corto periodo de tiempo, entonces el atacante no tiene una oportunidad para deducir la SRES y Kc a través de otros medios tal como la interpelación con RAND en el escenario GSM típico y atacar con el algoritmo A5/1 para deducir las claves.

La Figura 7 ilustra un procedimiento alternativo de realización de un protocolo de interpelación-respuesta entre un terminal móvil heredado (MT) 706 que soporta un Módulo de Identidad de Abonado 708 (SIM) de acuerdo con GSM y una función de servidor de secuencia inicial (BSF) 704 para autenticarse entre sí con seguridad y acordar una clave para funciones de aplicación de red (NAF) de acuerdo con una implementación. De modo similar al procedimiento de la Figura 6, se puede iniciar una solicitud de claves de autenticación por el MT 706 que envía su IMSI 700 asociado desde su SIM 708 a la BSF 704. La BSF 704 envía el IMSI 700 al HLR 702 por lo que puede verificar si el IMSI 700 pertenece a un MT que está abonado a la red. El HLR 702 selecciona y proporciona entonces el triplete (RAND, SERS, Kc) a la BSF 704, que corresponde a la identidad IMSI 700 del SIM 708. Por ejemplo, el RAND puede ser un número aleatorio de 128 bits y Ki es una clave de integridad secreta precompartida y se usan como entradas para los dos algoritmos A3 y A8 que producen una respuesta SRES firmada (por ejemplo número de 32 bits) y una clave Kc de confidencialidad secreta (por ejemplo un número de 64 bits), respectivamente. El MT 706 se supone que está provisto de una clave pública o certificado digital que le capacita para autenticar datos transmitidos desde la BSF 704.

La BSF 704 recibe el triplete (RAND, SRES, Kc) desde el HLR 702. La BSF 704 calcula entonces una firma digital SIG del RAND (y posiblemente otros parámetros, tal como un marcado de tiempos, número de secuencia, semilla aleatoria o información de identidad) usando un mecanismo basado en clave pública que capacita al MT 706 para autenticar el origen de los datos recibidos desde la BSF 704. La BSF 704 envía el RAND y SIG 710 al MT 706. Tras recibir el (RAND, SIG) 710, el MT 706 verifica el SIG usando el certificado digital de la BSF 704. Si se considera que los datos son de la BSF 704, el MT 706 envía el RAND 712 al SIM 708 para recuperar los parámetros SRES y Kc correspondientes. Esto es, el SIM 708 genera un par SRES y Kc mediante el uso de la clave secreta precompartida Ki y del RAND como entradas para los algoritmos A3 y A8 con los que se está provisto. El MT 706 puede generar entonces una clave PSK, cifrar la PSK bajo un mecanismo basado en clave pública y aplicar un código de autenticación del mensaje MAC al resultado. Se pueden incluir en la respuesta parámetros adicionales tal como un marcado de tiempos, número de secuencia, semilla aleatoria o información de identidad. El MAC se puede basar en una función o algoritmo (conocido tanto para el MT 706 como para la BSF 704) que puede incluir los Kc y SRES como parámetros de entrada y se usa para probar a la BSF 704 que el MT 706 posee la SIM 708 correcta. Nótese que las operaciones de cifrado basadas en clave pública de los datos y del MAC con las claves SRES y Kc se pueden realizar en cualquier orden. El MT 706 envía entonces el (PSK cifrado, MAC) 716 a la BSF 704, que verifica que el MT 706 está en posesión de los SRES y Kc correctos mediante la verificación del MAC. Esta verificación del MAC se realiza mediante el uso de los SRES y Kc recibidos por la BSF 704 desde el HLR 702 para recalcular un MAC y compararlo con el MAC recibido desde el MT 706. Si se considera que el MAC es correcto, se considera que el PSK se ha originado desde el MT 706 y la SIM 708 y se envía una confirmación o reconocimiento 718 al MT 706. De ese modo, este PSK se acuerda entre el MT 706 y la BSF 704 o se pueden realizar deducciones de claves adicionales usando los PSK, Kc, SRES, información de identidad y posiblemente otros parámetros.

El mecanismo de interpelación-respuesta ilustrado en las Figuras 6 y 7 para terminales móviles basados en GSM se puede implementar también en otros tipos de terminales móviles. Por ejemplo, la invención puede ser operativa en una red y terminales móviles (MT) de acuerdo con CDMA2000. En tal implementación, un terminal móvil de acuerdo con CDMA2000 contiene un módulo de autenticación cdma2000, UIM o RUIM para acordar una clave secreta precompartida que se puede usar para la seguridad de aplicaciones de red. En una implementación, la clave precompartida se puede generar usando un algoritmo de Diffie-Hellman autenticado, en el que un parámetro público P^x, proporcionado por la BSF se autentica por medio de un mecanismo de firma digital de clave pública (es decir un certificado del servidor de secuencia inicial conocido para el MT), mientras que el parámetro P^y, proporcionado por el MT, se autentica mediante la adición de un código de autenticación de mensaje cifrado con un material tal como SMEKEY (Clave de Cifrado de Mensaje de Señalización) desde el CAVE (Algoritmo de Autenticación Celular y Cifrado de Voz) o el Autenticador MN-AAA (Autenticación, Autorización y Contabilidad de Nodos Móviles). Se supone que el MT está provisto con una clave pública o certificado digital que lo capacita para autenticar mensajes firmados digitalmente desde la BSF y son conocidas una clave secreta Ki precompartida y un Identificador de Código de Autenticación IMSI tanto para el Módulo del Código de Autenticación como para el HLR.

Los expertos en la técnica apreciarán que este enfoque se aplica igualmente en circunstancias en las que la autenticación del portador se basa en CAVE y de nuevo ofrece la ventaja de que estas operaciones de secuencia inicial se pueden realizar usando en todo momento operaciones simétricas y RSA y puede ofrecer así ventajas de implementación sobre protocolos que requieran soporte tanto de Diffie-Hellman como de RSA.

Uno o más de los componentes y funciones ilustrados en las Figuras 1, 2 y/o 3 se pueden redisponer y/o combinar en un único componente o realizarse en varios componentes sin separarse de la invención. Se pueden añadir

elementos o componentes adicionales sin separarse de la invención. Los aparatos, dispositivos y/o componentes ilustrados en las Figuras 1, 2 y/o 3 se pueden configurar para realizar los procedimientos, características o etapas ilustradas en las Figuras 4, 5, 6 y/o 7.

Se debería tener en cuenta que las realizaciones precedentes son meramente ejemplos y no se deben interpretar como limitación de la invención. La descripción de las realizaciones tiene la finalidad de ser ilustrativa y no de limitar el alcance de las reivindicaciones. Como tales, las presentes enseñanzas se pueden aplicar fácilmente a otros tipos de aparatos y serán evidentes para los expertos en la técnica muchas alternativas, modificaciones y variaciones.

REIVINDICACIONES

1. Un procedimiento para la autenticación de una función de servidor de secuencia inicial (106, 604, 704) en un terminal móvil (102, 200, 606, 706) que soporta un módulo de identificación de abonado (204, 608, 708) heredado, que comprende:

- el aprovisionamiento del terminal móvil con un certificado digital asociado con la función de servidor de secuencia inicial;
- la recepción (404) de una interpelación de autenticación en el terminal móvil que incluye un número aleatorio;
- la autenticación, en el terminal móvil, de la función de servidor de secuencia inicial en base al certificado digital asociado con la función de servidor de secuencia inicial;
- que se provea con una primera clave secreta por el módulo de identificación de abonado heredado en respuesta al paso de un número aleatorio recibido en la interpelación de autenticación al módulo de identificación de abonado heredado;
- la formulación (510) de una respuesta de autenticación basada en la primera clave secreta proporcionada por el módulo de identificación de abonado heredado al terminal móvil.

2. El procedimiento de la reivindicación 1, que comprende además el envío de la respuesta de autenticación a la función de servidor de secuencia inicial para permitir a la función de servidor de secuencia inicial autenticar al terminal móvil.

3. El procedimiento de la reivindicación 1 o la reivindicación 2, en el que dicho aprovisionamiento permite que se realicen las comunicaciones desde la función de servidor de secuencia inicial al terminal móvil en un canal autenticado por el servidor.

4. El procedimiento de la reivindicación 1, 2 ó 3, que comprende además: el cálculo de una primera clave secreta en el módulo de identificación de abonado heredado usando el número aleatorio, una clave secreta precompartida y un algoritmo en el que la clave secreta precompartida y el algoritmo están ambos almacenados en el módulo de identificación de abonado heredado.

5. El procedimiento de cualquier reivindicación precedente, en el que la interpelación de autenticación recibida comprende además parámetros adicionales.

6. El procedimiento de la reivindicación 5, en el que la primera clave secreta se calcula usando los parámetros adicionales recibidos en la interpelación de autenticación.

7. El procedimiento de la reivindicación 2, que comprende además:

el cálculo de una clave adicional en el terminal móvil en base a la primera clave secreta,
en el que la clave adicional se calcula también independientemente en la función de servidor de secuencia inicial (106, 604, 704) en base a una segunda clave secreta proporcionada a la función de servidor de secuencia inicial por una base de datos (104, 602, 702) de red,
en el que la clave adicional se envía desde la función de servidor de secuencia inicial a una función de aplicación de red (108) solicitante de modo que el terminal móvil (102, 200, 606, 706) y la función de aplicación de red compartan la clave adicional.

8. El procedimiento de la reivindicación 7, en el que la clave adicional es una clave de aplicación, siendo deducida la clave de aplicación a partir de la clave compartida que se calcula en base a la primera clave secreta.

9. El procedimiento de cualquier reivindicación precedente, en el que el módulo de identificación de abonado (204, 608, 708) es o bien un Módulo de Identidad de Abonado, SIM; del Sistema Global para Móviles, GSM, o bien un Módulo de Autenticación del CDMA2000.

10. El procedimiento de cualquier reivindicación precedente en el que la interpelación de autenticación al terminal móvil se envía a través de un canal autenticado por el servidor.

11. El procedimiento de cualquier reivindicación precedente, en el que la interpelación de autenticación al terminal móvil incluye información de identidad.

12. Un terminal móvil (102, 200, 606, 706) que soporta un módulo de identificación de abonado (204, 608, 708) heredado, que comprende:

medios para recibir y almacenar un certificado digital asociado con una función de servidor de secuencia inicial (106, 604, 704);
medios para recibir una interpelación de autenticación desde una función de servidor de secuencia inicial en el terminal móvil que incluye un número aleatorio;
medios para la autenticación de la función de servidor de secuencia inicial en base al certificado digital asociado con la función de servidor de secuencia inicial;

medios para recibir una primera clave secreta desde el módulo de identificación de abonado heredado en respuesta al paso de un número aleatorio recibido en la interpelación de autenticación al módulo de identificación de abonado heredado y
medios para formular una respuesta de autenticación a la interpelación de autenticación basada en la primera clave secreta proporcionada por el módulo de identificación de abonado heredado al terminal móvil.

13. El terminal móvil de la reivindicación 12, que comprende además medios para el envío de la respuesta de autenticación a la función de servidor de secuencia inicial.

14. El terminal móvil de la reivindicación 12 o la reivindicación 13, que comprende además:

medios para el cálculo de la primera clave secreta en base a una clave secreta precompartida y a un algoritmo almacenados en el módulo de identificación de abonado heredado y al número aleatorio recibido en la interpelación de autenticación

15. El terminal móvil de la reivindicación 14, en el que la primera clave secreta se basa además en otros parámetros transmitidos en la interpelación de autenticación.

16. El terminal móvil de la reivindicación 14 o la reivindicación 15, que comprende además medios para el cálculo de un código de autenticación de mensajes usando la primera clave secreta y para la inclusión del código de autenticación de mensajes en la respuesta de autenticación.

17. El terminal móvil de cualquiera de las reivindicaciones 8 a 16 que comprende además:

una interfaz de comunicaciones inalámbrica para comunicarse con la función de servidor de secuencia inicial y
un circuito de procesamiento (202, 204) configurado para funcionar con un protocolo de comunicación heredado y autenticar el terminal móvil en un protocolo de respuesta a la interpelación con la función de servidor de secuencia inicial.

18. El terminal móvil de la reivindicación 10, en el que el circuito de procesamiento se configura para generar una clave adicional en base a la primera clave secreta.

19. El terminal móvil de la reivindicación 18, en el que la clave adicional se basa además en otros parámetros transmitidos en la interpelación de autenticación.

20. El terminal móvil de la reivindicación 18 o 19, en el que la clave adicional es una clave de aplicación que se basa en una clave compartida, siendo calculada la clave compartida mediante el uso de la primera clave secreta.

21. El terminal móvil de la reivindicación 18, 19 ó 20, en el que el circuito de procesamiento se configura además para generar un código de autenticación de mensajes.

22. El terminal móvil de la reivindicación 21, en el que la respuesta de autenticación incluye el código de autenticación de mensajes calculado usando la clave adicional.

23. El terminal móvil de cualquiera de las reivindicaciones 17 a 22, en el que el módulo de identificación de abonado heredado esta conectado al circuito de procesamiento y

el módulo de identificación de abonado heredado es para el almacenamiento de una clave secreta precompartida y un algoritmo.

24. El terminal móvil de la reivindicación 23 en el que el módulo de identificación de abonado heredado genera la primera clave secreta en base al número aleatorio, la clave secreta precompartida y el algoritmo.

25. El terminal móvil de la reivindicación 23 o la reivindicación 24, en el que el módulo de identificación de abonado heredado es un módulo de identidad de abonado de acuerdo con el protocolo del Sistema Global para Móviles, GSM.

26. El terminal móvil de la reivindicación 14, en el que la clave secreta precompartida se emplea también para permitir al terminal móvil establecer comunicaciones a través de una red inalámbrica heredada.

27. El terminal móvil de cualquiera de las reivindicaciones 12 a 26, en el que la interpelación de autenticación al terminal móvil se envía a través de un canal autenticado por el servidor.

28. El terminal móvil de cualquiera de las reivindicaciones 12 a 18, en el que la interpelación de autenticación al terminal móvil incluye información de identidad.

29. Un medio que pueda leer una máquina que lleve un producto de software que comprende segmentos de código que, cuando se ejecutan por un procesador, realiza el procedimiento de cualquiera de las reivindicaciones 1 a 11.

30. Un producto de software que comprende segmentos de código que, cuando se ejecutan por un procesador, realiza el procedimiento de cualquiera de las reivindicaciones 1-11.

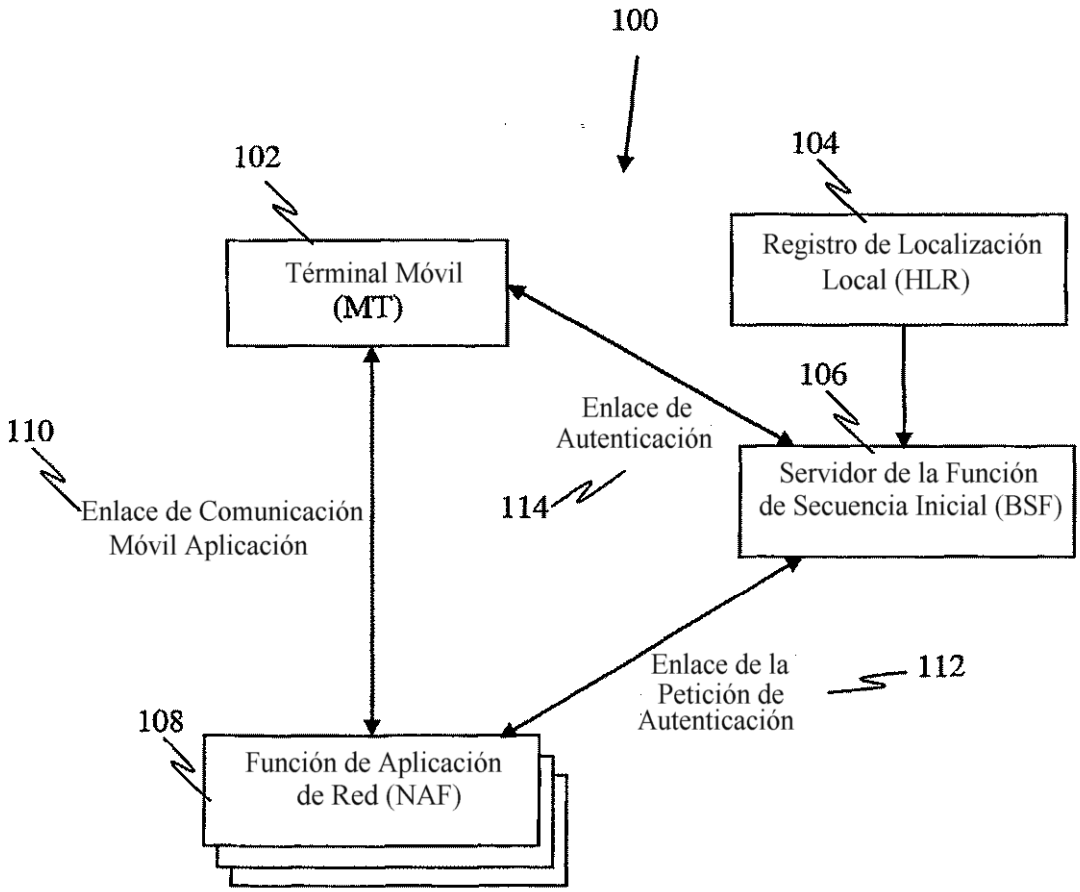
100
102
Términal Móvil
(MT)
104
Registro de Localización
Local (HLR)
106
Enlace de
Autenticación
114
110
Enlace de Comunicación
Móvil Aplicación
Servidor de la Función
de Secuencia Inicial (BSF)
Enlace de la
Petición de
Autenticación
112
108
Función de Aplicación
de Red (NAF)

Figura 1

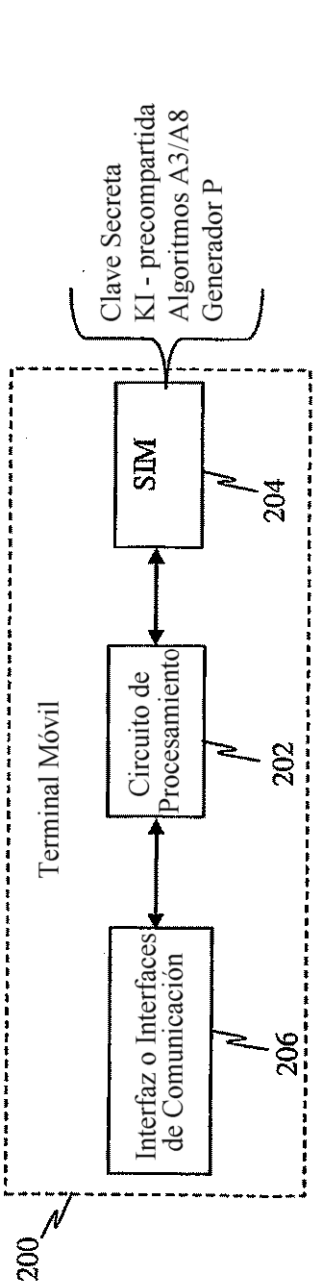

Figura 2

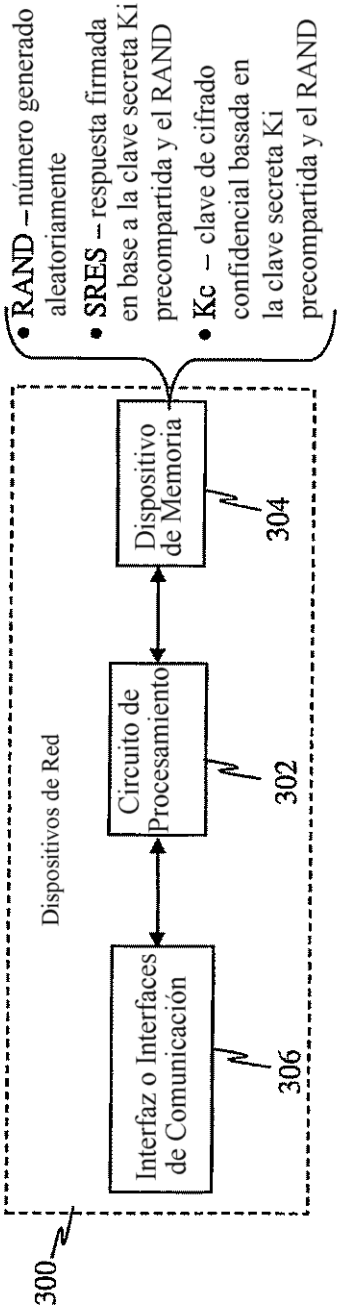

Figura 3

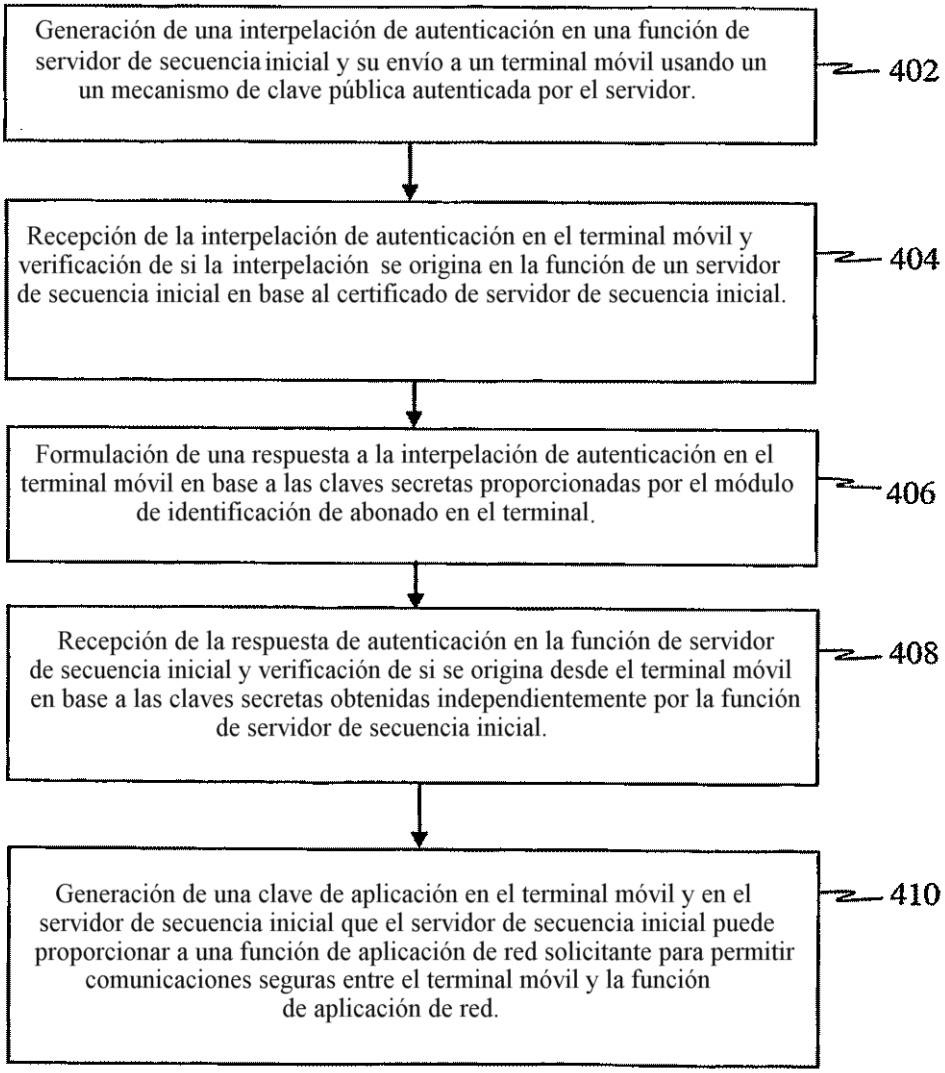
Generación de una interpelación de autenticación en una función de servidor de secuencia inicial y su envío a un terminal móvil usando un un mecanismo de clave pública autenticada por el servidor.
402
Recepción de la interpelación de autenticación en el terminal móvil y verificación de si la interpelación se origina en la función de un servidor de secuencia inicial en base al certificado de servidor de secuencia inicial.
404
Formulación de una respuesta a la interpelación de autenticación en el terminal móvil en base a las claves secretas proporcionadas por el módulo de identificación de abonado en el terminal.
406
Recepción de la respuesta de autenticación en la función de servidor de secuencia inicial y verificación de si se origina desde el terminal móvil en base a las claves secretas obtenidas independientemente por la función de servidor de secuencia inicial.
408
Generación de una clave de aplicación en el terminal móvil y en el servidor de secuencia inicial que el servidor de secuencia inicial puede proporcionar a una función de aplicación de red solicitante para permitir comunicaciones seguras entre el terminal móvil y la función de aplicación de red.
410

Figura 4

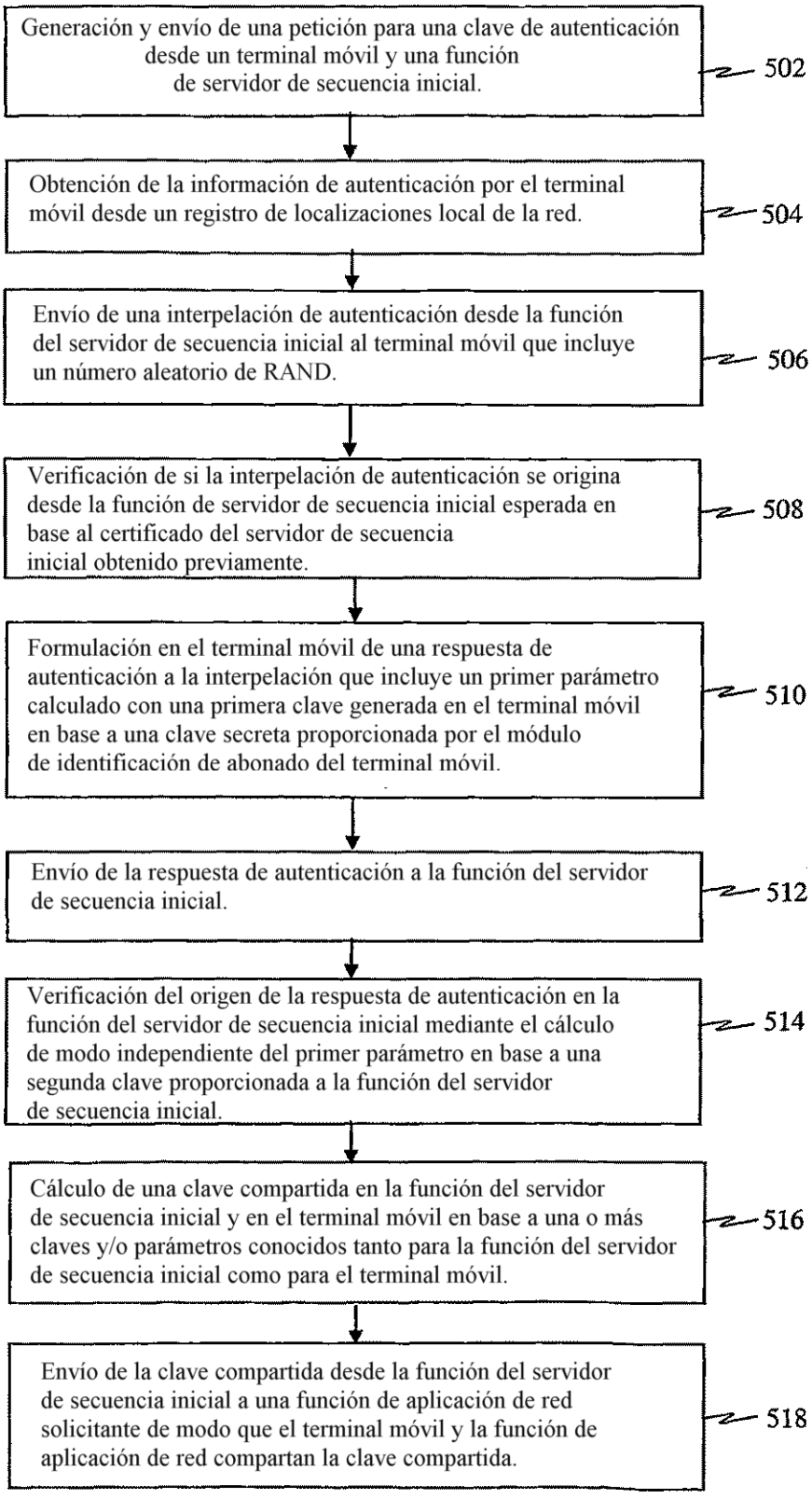
Generación y envío de una petición para una clave de autenticación desde un terminal móvil y una función de servidor de secuencia inicial.
502
Obtención de la información de autenticación por el terminal móvil desde un registro de localizaciones local de la red.
504
Envío de una interpelación de autenticación desde la función del servidor de secuencia inicial al terminal móvil que incluye un número aleatorio de RAND.
506
Verificación de si la interpelación de autenticación se origina desde la función de servidor de secuencia inicial esperada en base al certificado del servidor de secuencia inicial obtenido previamente.
508
Formulación en el terminal móvil de una respuesta de autenticación a la interpelación que incluye un primer parámetro calculado con una primera clave generada en el terminal móvil en base a una clave secreta proporcionada por el módulo de identificación de abonado del terminal móvil.
510
Envío de la respuesta de autenticación a la función del servidor de secuencia inicial.
512
Verificación del origen de la respuesta de autenticación en la función del servidor de secuencia inicial mediante el cálculo de modo independiente del primer parámetro en base a una segunda clave proporcionada a la función del servidor de secuencia inicial.
514
Cálculo de una clave compartida en la función del servidor de secuencia inicial y en el terminal móvil en base a una o más claves y/o parámetros conocidos tanto para la función del servidor de secuencia inicial como para el terminal móvil.
516
Envío de la clave compartida desde la función del servidor de secuencia inicial a una función de aplicación de red solicitante de modo que el terminal móvil y la función de aplicación de red compartan la clave compartida.
518

Figura 5

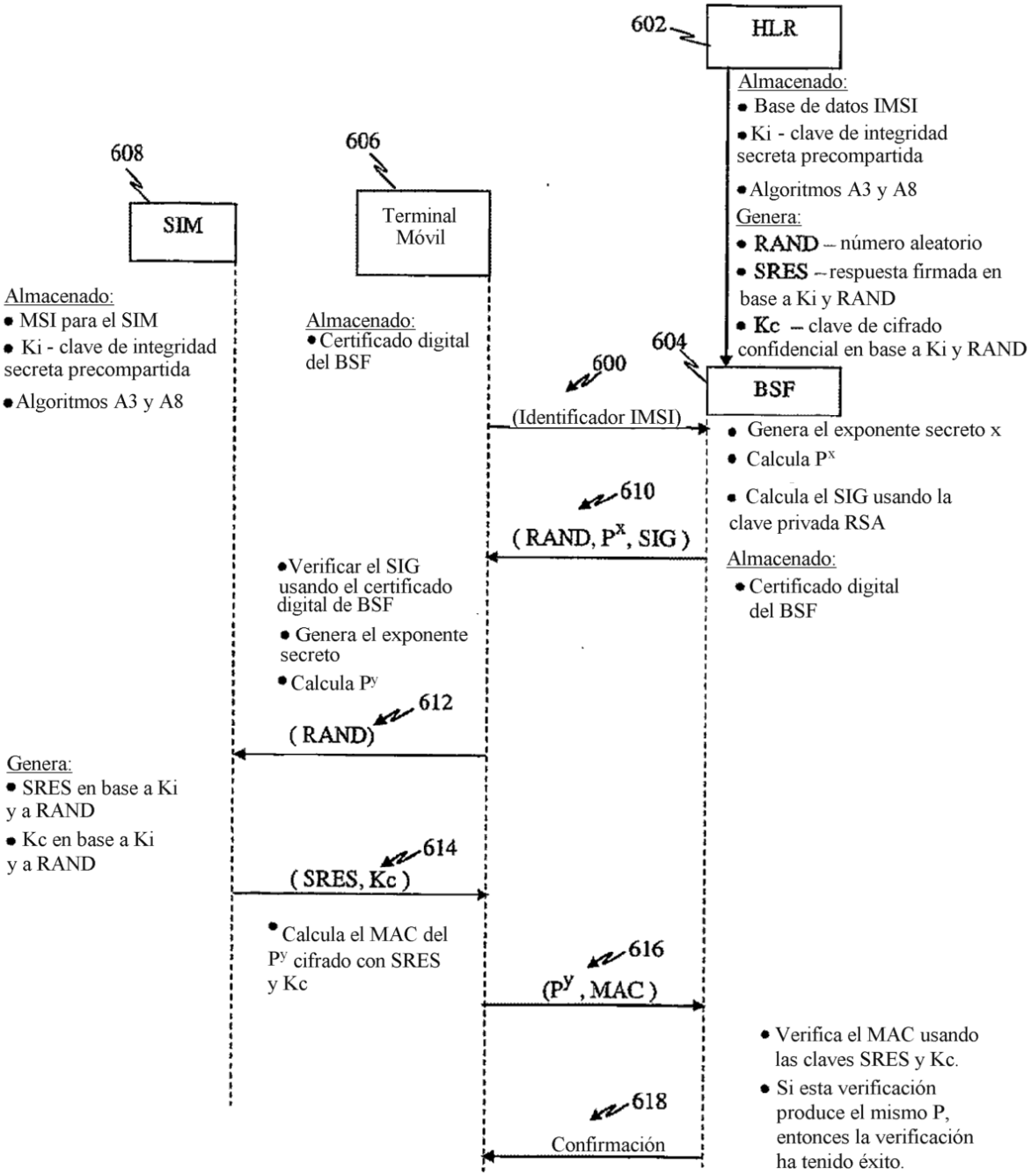
602
HLR
Almacenado:
• Base de datos IMSI
• Ki - clave de integridad secreta precompartida
• Algoritmos A3 y A8
Genera:
• RAND – número aleatorio
• SRES – respuesta firmada en base a Ki y RAND
• Kc – clave de cifrado confidencial en base a Ki y RAND
608
SIM
606
Terminal Móvil
604
BSF
Almacenado:
• MSI para el SIM
• Ki - clave de integridad secreta precompartida
• Algoritmos A3 y A8
Almacenado:
• Certificado digital del BSF
600
(Identificador IMSI)
• Genera el exponente secreto x
• Calcula P^x
• Calcula el SIG usando la clave privada RSA
610
(RAND, P^x, SIG)
Almacenado:
• Certificado digital del BSF
• Verificar el SIG usando el certificado digital de BSF
• Genera el exponente secreto
• Calcula P^y
612
(RAND)
Genera:
• SRES en base a Ki y a RAND
• Kc en base a Ki y a RAND
614
(SRES, Kc)
• Calcula el MAC del P^y cifrado con SRES y Kc
616
(P^y , MAC)
• Verifica el MAC usando las claves SRES y Kc.
• Si esta verificación produce el mismo P, entonces la verificación ha tenido éxito.
618
Confirmación

Figura 6

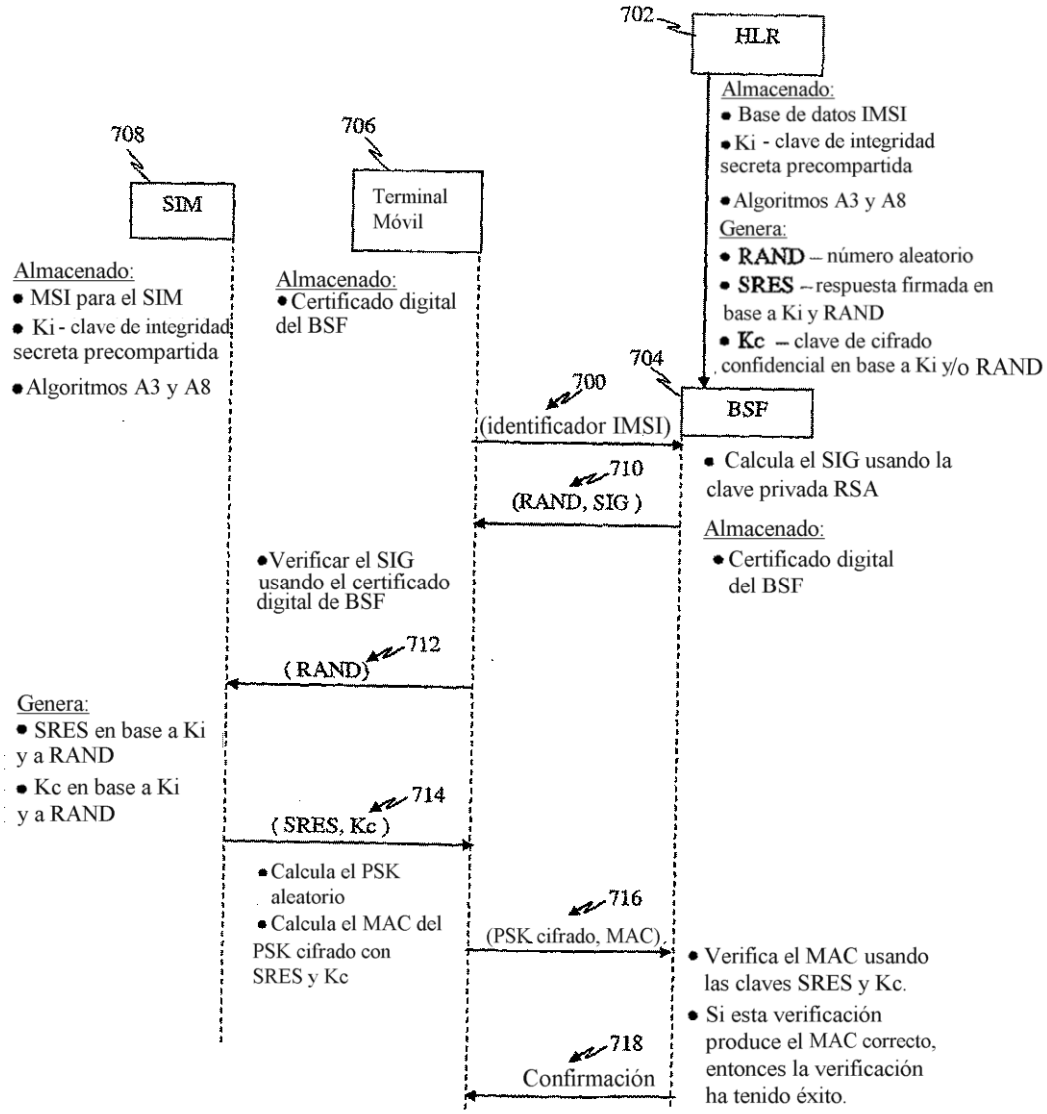
702
HLR
Almacenado:
• Base de datos IMSI
• Ki - clave de integridad secreta precompartida
• Algoritmos A3 y A8
Genera:
• RAND – número aleatorio
• SRES – respuesta firmada en base a Ki y RAND
• Kc – clave de cifrado confidencial en base a Ki y/o RAND
708
SIM
706
Terminal Móvil
704
BSF
Almacenado:
• MSI para el SIM
• Ki - clave de integridad secreta precompartida
• Algoritmos A3 y A8
Almacenado:
• Certificado digital del BSF
700
(identificador IMSI)
• Calcula el SIG usando la clave privada RSA
710
(RAND, SIG)
Almacenado:
• Certificado digital del BSF
• Verificar el SIG usando el certificado digital de BSF
712
(RAND)
Genera:
• SRES en base a Ki y a RAND
• Kc en base a Ki y a RAND
714
(SRES, Kc)
• Calcula el PSK aleatorio
• Calcula el MAC del PSK cifrado con SRES y Kc
716
(PSK cifrado, MAC)
• Verifica el MAC usando las claves SRES y Kc.
• Si esta verificación produce el MAC correcto, entonces la verificación ha tenido éxito.
718
Confirmación

Figura 7