(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 807 532**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 29/06 (2006.01)
H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.03.2007 E 17154410 (9)**

(97) Fecha y número de publicación de la concesión europea: **06.05.2020 EP 3182639**

(54) Título: **Un método y aparato para manejar claves para encriptación e integridad**

(30) Prioridad:

28.03.2006 SE 0600695
28.03.2006 US 786478 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.02.2021

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

NÄSLUND, MATS;
NORRMAN, KARL y
BLOM, ROLF

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Un método y aparato para manejar claves para encriptación e integridad

Campo técnico

La presente invención se refiere en general a un método y aparato para proporcionar claves para proteger la comunicación entre un terminal y puntos de servicio en una red de comunicación.

Antecedentes

En la comunicación inalámbrica, la seguridad es un tema importante ya que transmitir información por el aire hace posible interceptar y/o modificar ilícitamente la información comunicada. Por lo tanto, la información generalmente está encriptada y/o con protección de integridad antes de ser enviada por aire. Los estándares de comunicación que prevalecen hoy en día para la comunicación por radio implican varios métodos y rutinas de seguridad. Por ejemplo, las redes de acceso móviles (o celulares) de acuerdo con GSM (sistema global para comunicaciones móviles), GPRS (servicio general de radio por paquetes) y UMTS (sistema universal de telecomunicaciones móviles) utilizan dos claves denominadas Ck e Ik, para garantizar la integridad y para encriptar información comunicada por canales de radio entre un terminal móvil particular y la red móvil.

En UMTS, cada terminal móvil comparte un par único de claves Ck e Ik con la red que puede usarse para encriptar datos de carga útil, así como varios mensajes de señalización, y también para verificar la identidad del terminal, denominada integridad. Las claves Ck e Ik que se usarán en una sesión se establecen durante una etapa de registro cuando el terminal se conecta a la red, que se denominará acuerdo de clave en esta descripción. Cabe señalar que un terminal móvil puede estar en dos modos diferentes, denominado modo inactivo cuando se ha registrado como presente en la red pero no está involucrado en una sesión de transmisión/recepción de datos, y el modo activo cuando transmite/recibe datos en una sesión.

La información comunicada por aire entre un terminal móvil y una estación base se divide convencionalmente en tres categorías principales: 1) datos de carga útil, también conocidos como datos de "plano de usuario", 2) señalización NAS (estrato de no acceso) que es información relacionado, por ejemplo, con la seguridad, incluida la autenticación y la encriptación, y 3) RRC (control de recursos de radio) que es información relacionada con la comunicación por radio, incluidos los detalles del canal, esquemas de modulación y multiplexación, regulación de potencia, mediciones de señal, etc.

En los llamados sistemas 3G de acuerdo con UMTS, los datos del plano de usuario se transmiten típicamente a través de cuatro nodos diferentes en la red de acceso: la estación base (también conocida como NodoB), el RNC (controlador de red de radio), el SGSN (nodo de soporte GPRS de servicio) y el GGSN (nodo de soporte GPRS de pasarela), del cual las estaciones base y RNC constituyen una parte de la red de radio y el SGSN y GGSN constituyen una parte de la red central. En los sistemas 3G, toda la encriptación/desencriptación de los datos del plano de usuario, NAS y RRC se ejecutan por el RNC y el terminal, mientras que en los sistemas GSM tradicionales, la encriptación es manejada por las estaciones base.

Actualmente, se está desarrollando una nueva arquitectura de red para proporcionar el llamado "acceso 3G evolucionado", como se ilustra en la figura 1, basado en 3GPP (proyecto de asociación de tercera generación). La nueva arquitectura comprende básicamente dos tipos de nodos que incluyen estaciones base "evolucionadas" 100 en la parte de la red de radio conectada a una pasarela central 102 de enlace de control de acceso AGW en la parte de la red central por medio de la conocida interfaz S1. Una red de acceso puede contener varios nodos AGW que sirven a diferentes áreas geográficas. El nodo AGW está conectado a varias redes externas diferentes 104 usando interfaces bien conocidas, incluyendo Internet (usando la interfaz Gi), otras redes 3GPP (usando la interfaz Gn) y redes no 3GPP (usando la interfaz S2), e incluye ciertas funciones similares a las implementadas actualmente en el RNC, SGSN y GGSN.

En particular, el procesamiento de seguridad relacionado con la encriptación y la integridad tendrá lugar en la estación base 100 y el nodo AGW 102. Básicamente, la encriptación de los datos del plano del usuario, y potencialmente también la señalización NAS, será manejado por el nodo AGW 102, mientras que la protección de la señalización RRC será manejada por las estaciones base 100. El proceso inicial de autenticación del abonado y el acuerdo clave tendrá lugar entre un SIM (módulo de identidad del abonado) en el terminal y el nodo AGW, y a menudo se lo conoce como AKA (acuerdo de autenticación y clave). Por lo tanto, las claves mencionadas anteriormente Ck e Ik pueden ser establecidas por el terminal y el nodo AGW durante el proceso AKA.

Para proporcionar interoperabilidad entre diferentes arquitecturas de red, es altamente deseable que los componentes de seguridad y las rutinas de los sistemas 3G existentes puedan reutilizarse también en la arquitectura de dos nodos descrita anteriormente, incluido el mantenimiento del proceso AKA. En consecuencia, existe la necesidad de proporcionar claves de seguridad tanto para la estación base como para el nodo AGW, preferiblemente basadas en las claves anteriores Ck e Ik. En la estación base se necesita una clave para proteger la

señalización RRC, y en el nodo AGW se necesita una clave para proteger la señalización NAS así como los datos del plano de usuario.

Aunque sería posible enviar una copia de, por ejemplo, Ik a la estación base y usar la misma clave tanto en la estación base como en el nodo AGW, esto puede dar lugar a ciertos inconvenientes. En primer lugar, una estación base local es algo vulnerable a los ataques ilícitos al estar situada típicamente en lugares de fácil acceso y sin vigilancia, en comparación con el nodo AGW más centralizado que se puede instalar totalmente protegido. Por lo tanto, existe el riesgo de que la clave Ik sea interceptada en la estación base de modo que la señalización NAS se pueda detectar de forma ilícita. Cabe señalar en este contexto que la información NAS confidencial generalmente exige un mayor grado de seguridad que la información RRC. Sin embargo, la señalización RRC puede incluir un identificador de terminal que hace que sea deseable proteger de todos modos.

En segundo lugar, puede ser difícil obtener una protección satisfactoria para el caso cuando la información interceptada se graba y se reproduce más tarde (los llamados ataques de repetición), si la misma clave se usa para dos propósitos diferentes que brindan múltiples oportunidades para detectar la clave usada. Por lo tanto, si Ik se reutiliza en la estación base, se requiere que el nodo AGW al menos aplique alguna función unidireccional f a Ik antes de enviarlo en una forma modificada f (Ik) = Ik' a la estación base.

Sin embargo, si Ik' es interceptado en una estación base durante una sesión, este fallo de seguridad persistirá incluso si la sesión se traspasa a una nueva estación base, es decir, siempre que se use Ik'. Este problema se puede evitar si el proceso AKA se repite a intervalos regulares (por ejemplo, desencadenado por el traspaso), lo que, sin embargo, puede perturbar la sesión y, por lo tanto, afectar significativamente a un comportamiento deseable de los servicios.

Por lo tanto, es deseable evitar la inseguridad persistente después de una intercepción de claves a medida que el terminal se mueve entre diferentes puntos de servicio, es decir, estaciones base, pero sin requerir operaciones adicionales como el establecimiento de nuevas claves en una reautenticación de acuerdo con el proceso AKA. Se ha hecho un intento por cumplir estos objetos con un nuevo tipo de clave que se comparte entre la estación base y el nodo AGW, de acuerdo con un procedimiento propuesto que se describe a continuación con referencia a la figura 2.

La figura 2 ilustra un terminal móvil 200 y una red de acceso móvil que incluye una pluralidad de estaciones base de las cuales se muestran dos, BS1 202 y BS2 204, que están conectadas a un nodo AGW central 206, de acuerdo con la arquitectura de dos nodos mostrada en la figura 1. En esta propuesta, cada estación base en la red cubierta por el nodo AGW 206 comparte una clave predefinida con el nodo AGW. Como se indica en la figura, las estaciones base 202 y 204 comparten las claves predefinidas k1 y k2, respectivamente, con el nodo AGW 206.

Primero, el terminal 200 se conecta a la red por conexión de radio con BS1 202, siendo así la estación base de servicio, y las claves convencionales Ck e Ik se establecen mediante el proceso AKA, en un primer paso 2:1.

Para establecer una mayor protección, el nodo AGW 206 buscará la clave k1 de BS1. Además, el nodo AGW también buscará la clave correspondiente de un número adecuado de estaciones base "vecinas", es decir, estaciones base ubicadas en la vecindad de la estación base BS1 de servicio a la que se podría traspasar el terminal cuando se mueva durante una sesión, incluyendo BS2 204. Las estaciones base vecinas deben seleccionarse para cubrir un área razonable en la que se espera que esté el terminal. Alrededor de 5 a 10 estaciones base pueden considerarse estaciones base vecinas, por ejemplo, dependiendo de sus tamaños de celda.

A continuación, el nodo AGW 206 usa la clave Ik establecida para el terminal 200, para crear una clave modificada específicamente para cada estación base, aplicando una función f predeterminada con la clave Ik y una identidad de estación base "BS" como entrada, como sigue: Ik_1 = f(Ik, "BS1") se crea para BS1, Ik_2 = f(Ik, "BS2") se crea para BS2 y, en general, Ik_j = f(Ik, "BSj") se crea para la estación base j. Cabe señalar que la función f predeterminada también es conocida por el terminal, que se utilizará como se describe a continuación.

Cada clave Ik Ik_1, Ik_2 ... Ikj modificada producida es luego "envuelta" (es decir, encriptada) por la clave k compartida con la estación base correspondiente, formando un conjunto de claves envueltas individualmente para todas las estaciones base (la de servicio y las vecinas): Encr (k1, Ik_1), Encr (k2, Ik_2) ... Encr (kj, Ik_j). A continuación, "K" se usará para abreviar para representar el conjunto completo de todas estas claves envueltas. Todo el proceso de creación de K como se describió anteriormente se ilustra en el paso 2:2 de la figura.

De acuerdo con el procedimiento propuesto, el nodo AGW 206 ahora transfiere todo el conjunto de claves K a la estación base BS1 202 de servicio, en el siguiente paso 2:3. BS1 puede desencriptar el componente de K correspondiente a Encr (k1, Ik_1) usando su clave única k1, para extraer la clave Ik Ik_1 modificada mencionada anteriormente originalmente creada para esa estación base, en un paso siguiente 2:4, para ser compartida con el terminal. BS1 también almacena todo el conjunto de claves K para su futuro uso.

Dado que el terminal conoce naturalmente su clave Ik original y la identidad de la estación base "BS1" de servicio, puede derivar la misma clave Ik Ik_1 modificada aplicando la función f: Ik_1 = f (Ik, "BS1"), en conexión con el inicio de

una sesión de comunicación, como se muestra en el paso 2:5. Por lo tanto, ahora se ha establecido una clave modificada Ik_1 que es única para esta combinación particular de terminal y estación base, basada en la clave única de terminal Ik y la identidad única de estación base "BS1". La clave Ik1 ahora puede ser usada por el terminal 200 y la estación base 202 para proteger la señalización RRC durante la sesión, siempre que el terminal 200 permanezca conectado a la estación base 202.

Si el terminal en algún momento durante la sesión se mueve para ser traspasado a una nueva estación base, en este caso BS2 204 como se ilustra con la flecha discontinua, el viejo BS1 202 transfiere todo el conjunto de claves K a BS2 204, en el paso 2:6. Usando el conjunto de claves K recibido, BS2 204 puede extraer de manera similar su propia clave Ik Ik_2 modificada en el paso 2:7. El terminal también derivará Ik_2 usando la función f (Ik, "BS2"), en el paso 2:8, que se usará como clave para la encriptación y/o integridad en futuras comunicaciones.

El procedimiento propuesto descrito anteriormente para establecer una clave Ik modificada también se puede usar para establecer una clave Ck modificada que sea única para cada combinación particular de terminal y estación base, a fin de proporcionar una protección más confiable de la comunicación del plano de usuario y la señalización NAS sensible.

Por lo tanto, la solución de la técnica anterior descrita anteriormente proporciona claves únicas para cada combinación de estación base-terminal. Incluso si en algún momento se intercepta ilícitamente una clave Ik_x usada en una celda x (es decir, la estación base), se usará una nueva clave Ik_y en cuanto se traspase a otra celda y el fallo de seguridad no persista. Por lo tanto, la solución en la figura 2 proporciona seguridad tanto hacia atrás como hacia adelante cada vez que se cambia la estación base de servicio.

Se divulgan otras soluciones de la técnica anterior en los documentos: WO 2005/032201 A1 y US 2005/0031126 A1.

Sin embargo, hay algunos problemas importantes asociados con la solución anterior. En general, es bastante complejo ya que las nuevas claves Ik deben calcularse y envolverse para un número significativo de estaciones base, de las cuales solo se usarán unas pocas, si es que las hay. Además, el nodo AGW necesita "predecir" qué estaciones base podrían estar involucradas en futuros traspasos, lo cual es más o menos casual ya que el terminal puede moverse en direcciones inesperadas. Si el terminal se mueve rápidamente fuera del área cubierta por la colección de estaciones base vecinas seleccionadas incluidas en el conjunto de claves K, el proceso debe comenzar de nuevo para obtener un conjunto de claves K para una nueva área. Además, se requiere que las estaciones base de servicio almacenen todo el conjunto de claves K, y no solo su clave "propia", y que lo transfieran a la siguiente estación base tras el traspaso.

En general, es deseable obtener una forma simple pero confiable de usar claves para la encriptación y/o con protección de integridad, particularmente cuando un terminal de comunicación conmuta la comunicación de un punto de servicio a otro. Más específicamente, sería beneficioso evitar la necesidad de predicciones de traspaso y reducir la cantidad de claves que deben manejar las estaciones base u otros puntos de servicio. También es deseable proporcionar seguridad hacia atrás al conmutar los puntos de servicio y seguridad hacia adelante cuando un terminal inicia una sesión, por ejemplo, pasa del modo inactivo al modo activo, con un mínimo impacto en el servicio.

Aunque la descripción de antecedentes se ha centrado en terminales móviles que usan estaciones base en una red 3G como puntos de servicio, los temas discutidos también pueden ser relevantes para otras redes de acceso móviles (o celulares), y también para redes de acceso fijo que usan conexiones cableadas como como DSL (línea de abonado digital), PON (red óptica pasiva) y DOCSIS (especificación de interfaz de servicio de datos por cable). Por ejemplo, el proceso AKA mencionado anteriormente puede ser reemplazado por otros procesos similares para establecer una o más claves para ser usadas en las comunicaciones de sesión, dependiendo de las rutinas de red prevalecientes. Además, viendo el "acceso" o la "conectividad" como un servicio general, la presente invención también se puede aplicar a otros servicios de comunicación, por ejemplo, transmisión de datos, etc.

Sumario

Es un objeto de la presente invención abordar en general los problemas y demandas descritos anteriormente, y proporcionar un mecanismo conveniente para obtener claves para proteger la comunicación entre un terminal y puntos de servicio en una red de comunicación.

Este objeto y otros pueden obtenerse por métodos y disposiciones, respectivamente, de acuerdo con las reivindicaciones independientes adjuntas.

En la presente invención, se definen un método y una disposición para proporcionar claves para proteger la comunicación entre un terminal y puntos de servicio en una red de comunicación, tal como se implementa en un nodo de control de servicio. Primero se establece una clave básica para el terminal durante un procedimiento de registro cuando el terminal ha entrado en la red. Luego se crea una clave modificada inicial aplicando una función predeterminada al menos a la clave básica y a un valor inicial de un parámetro de versión de clave, cuando el terminal inicia una primera sesión de comunicación. La clave modificada inicial se envía a un primer punto de

servicio al que se conecta inicialmente el terminal, de modo que se puede usar para proteger la comunicación entre el terminal y el primer punto de servicio.

En una etapa posterior, se puede recibir una solicitud de clave desde un nuevo punto de servicio al que está conectado el terminal, por ejemplo, cuando el terminal entra en un estado activo después de un período en estado inactivo. En respuesta a esto, se crea una nueva clave modificada inicial aplicando dicha función al menos a la clave básica y a un valor actualizado de dicho parámetro de versión de clave, cuando el terminal inicia una segunda sesión de comunicación. La nueva clave modificada inicial se envía finalmente al nuevo punto de servicio, de modo que se puede usar para proteger la comunicación entre el terminal y el nuevo punto de servicio.

También se puede introducir una identidad de punto de servicio a la función predeterminada al crear la clave modificada inicial y/o la nueva clave modificada inicial, para hacer que la clave sea única para la combinación particular de terminal/punto de servicio.

El valor del parámetro de versión de clave se inicializa a un cierto valor y luego se cambia de acuerdo con un esquema o algoritmo predeterminado cada vez que se crea una nueva clave modificada inicial. Por ejemplo, el parámetro de versión de clave puede inicializarse a cero y luego incrementarse en uno cada vez que se crea una nueva clave modificada inicial.

La solicitud de clave puede recibirse cuando el terminal se reactiva después de estar inactivo, o después de que el terminal ha estado activo un período de tiempo preestablecido, o ha comunicado una cantidad predeterminada de datos, o ha realizado un número predeterminado de conmutaciones de punto de servicio.

También se definen un método y una disposición para obtener claves para proteger la comunicación con un terminal inicialmente conectado a un punto de servicio en una red de comunicación, tal como se ejecuta en dicho punto de servicio. En el punto de servicio, se recibe primero una clave modificada inicial desde un nodo de control de servicio, que se ha creado aplicando una primera función predeterminada al menos a una clave básica establecida para el terminal y un valor inicial de un parámetro de versión de clave. Cuando se detecta que el terminal conmutará a un segundo punto de servicio durante una sesión en curso, se crea una segunda clave modificada aplicando una segunda función predeterminada al menos a la clave modificada inicial. La segunda clave modificada se envía finalmente al segundo punto de servicio, de modo que se puede usar para proteger la comunicación entre el terminal y el segundo punto de servicio.

El punto de servicio puede enviar una solicitud de clave al nodo de control de servicio para obtener una nueva clave modificada inicial. La solicitud de clave puede enviarse cuando el terminal se reactiva después de estar inactivo, o después de que el terminal ha estado activo un período de tiempo preestablecido, o ha comunicado una cantidad predeterminada de datos, o ha realizado un número predeterminado de conmutaciones de punto de servicio.

Un método y una disposición se definen además para obtener claves para proteger la comunicación con puntos de servicio en una red de comunicación, tal como se ejecuta en un terminal inicialmente conectado a un primer punto de servicio en la red. Una clave básica Ik se determina por primera vez durante un procedimiento de registro al entrar en la red. Luego, se crea una clave modificada inicial aplicando una primera función predeterminada al menos a la clave básica y a un valor inicial de un parámetro de versión de clave, al iniciar una primera sesión de comunicación, de modo que se pueda usar para proteger la comunicación con el primer punto de servicio. Si el terminal conmuta a un segundo punto de servicio, se crea una segunda clave modificada aplicando una segunda función predeterminada al menos a la clave modificada inicial.

Si el terminal se conecta a un nuevo punto de servicio después de un período de inactividad para comenzar una segunda sesión de comunicación, se crea una nueva clave modificada inicial aplicando nuevamente la primera función al menos a la clave básica y a un valor actualizado de dicho parámetro de versión de clave, de modo que pueda usarse para proteger la comunicación con el nuevo punto de servicio.

También se puede introducir una identidad de punto de servicio a la función predeterminada al crear la clave modificada inicial y/o la nueva clave modificada inicial, para hacer que la clave sea única para la combinación particular de terminal/punto de servicio.

El valor del parámetro de versión de clave se inicializa primero a un cierto valor y luego se cambia de acuerdo con un esquema o algoritmo predeterminado cada vez que se crea una nueva clave modificada inicial. Por ejemplo, el parámetro de versión de clave puede inicializarse a cero y luego incrementarse en uno cada vez que se crea una nueva clave modificada inicial.

Breve descripción de los dibujos

La presente invención se describirá ahora con más detalle y con referencia a los dibujos adjuntos, en los que:

- la figura 1 es una vista esquemática que ilustra una arquitectura de red móvil de acuerdo con un acceso 3G evolucionado propuesto previamente conocido para comunicación móvil, en el que se puede usar la presente invención.

- la figura 2 es un diagrama de bloques esquemático que ilustra un procedimiento propuesto para manejar claves en la arquitectura de red mostrada en la figura 1, de acuerdo con la técnica anterior.

- la figura 3A es un diagrama de señalización que ilustra un procedimiento de manejo de claves, de acuerdo con una realización.

- la figura 3B es un diagrama de señalización que ilustra un procedimiento de manejo de claves, continuado de la figura 3A.

- la figura 3C es un diagrama de señalización que ilustra un procedimiento de manejo de claves, continuado de la figura 3B.

- la figura 4 es un diagrama de flujo que ilustra un procedimiento básico para proporcionar claves, tal como se ejecuta en un nodo de control de servicio, de acuerdo con otra realización.

- la figura 5 es un diagrama de flujo que ilustra un procedimiento básico para obtener claves, tal como se ejecuta en un punto de servicio, de acuerdo con otra realización más.

- la figura 6 es un diagrama de flujo que ilustra un procedimiento básico para obtener claves, tal como se ejecuta en un terminal, de acuerdo con otra realización más.

Descripción de realizaciones preferidas

Una realización de la presente invención se describirá ahora inicialmente con referencia a la figura 3A, que es un diagrama de señalización que ilustra una primera fase en un procedimiento de manejo de claves para la encriptación y/o integridad en una red de acceso de comunicación, por ejemplo, la red de acceso móvil que se muestra en la figura 1.

La figura 3A ilustra un terminal 300 de comunicación, un primer punto 302 de servicio y un nodo 304 de control de servicio al que está conectado el primer punto 302 de servicio, así como una pluralidad de otros puntos de servicio (no mostrados). En la práctica, el terminal 300 puede ser un terminal móvil, el primer punto 302 de servicio puede ser una estación base, y el nodo 304 de control de servicio puede ser una AGW, como se describió anteriormente. En esta descripción, el término "nodo de control de servicio" generalmente puede representar cualquier nodo de red central, por ejemplo, en una red central, controlando un servicio de telecomunicaciones que se ejecuta cuando el terminal está conectado a un punto de servicio.

Un primer paso 3:1 ilustra que al menos una clave básica para la encriptación y/o integridad se establece entre el terminal 300 y el nodo 304 de control de servicio, por ejemplo, de acuerdo con una rutina convencional tal como el procedimiento AKA cuando un terminal móvil se conecta inicialmente a una estación base, es decir, el punto 302 de servicio. Esta clave básica se denota aquí Ik en analogía con el procedimiento propuesto de la figura 2, aunque otras claves como Ck también se pueden usar en la presente solución. Además, la presente solución se puede aplicar para cualquier número de claves que puedan emplearse para diferentes propósitos, tales como encriptación, integridad, autenticación, etc., pero solo una clave Ik se describirá en esta realización por simplicidad.

Como se ilustra en un paso siguiente 3:2, el nodo 304 de control de servicio crea una clave modificada inicial Ik_1 mediante la aplicación de una primera función f predeterminada al menos a la clave original Ik y opcionalmente también una identidad de punto de servicio "SP1" para hacer que la clave Ik1 sea única para esta combinación de terminal/punto de servicio, similar a la creación de claves modificadas en la propuesta de la figura 2. Aquí también se pueden usar otros parámetros como entrada a la función f, como otras claves básicas (por ejemplo, Ck) y una identidad terminal, que sin embargo está fuera del alcance de la presente invención.

En la presente solución, se introduce un parámetro de versión de clave v como entrada adicional a la función f para indicar la versión actual de la clave modificada inicial Ik_1, de modo que Ik_1 = f(Ik, v). Como se mencionó anteriormente, "SP1" y/u otros parámetros también pueden usarse como entrada a la función f. El valor del parámetro de versión de clave v se cambiará de acuerdo con un esquema predeterminado cada vez que se crea una clave modificada Ik_1 como se describe a continuación, aquí indicado como v, v', v", v"', etc. Por ejemplo, el parámetro de clave de versión v puede inicializarse en v = 0 (cero) y luego simplemente incrementarse en uno tal que v '= 1, v" = 2, v"' = 3, etc., que se usa en la presente realización. Sin embargo, el valor del parámetro de versión de clave v se puede cambiar de acuerdo con cualquier esquema o algoritmo concebible, y la presente solución no está limitada a este respecto. Cabe señalar que el valor actual del parámetro v y la función f deben ser conocidos tanto por el terminal 300 como por el nodo 304 de control de servicio.

Volviendo a la figura 3A, el nodo 304 de control de servicio envía la clave modificada inicial Ik_1 al punto 302 de servicio en un paso siguiente 3:3, para usar en cualquier comunicación próxima con el terminal 300. Al mismo tiempo, el terminal 300 puede derivar la misma clave modificada inicial Ik_1 aplicando la función f (Ik, v) en conexión con el inicio de una sesión de comunicación, como se ilustra en el paso 3:4. Cabe señalar que el terminal 300 puede ejecutar el paso 3:4 en cualquier momento después del paso 3:1, es decir, independiente de los pasos 3:2 y 3:3. La clave Ik_1 ahora puede ser usada por el terminal 300 y el punto 302 de servicio para proteger cualquier comunicación durante la sesión, siempre que el terminal 300 permanezca conectado al punto 302 de servicio, como se ilustra en el paso 3:5. En este paso, "(Datos) Ik_1" generalmente indica que los datos comunicados están protegidos por Ik_1.

Hablando en términos generales, cualquier tipo de comunicación puede protegerse de cualquier manera por medio de la clave Ik_1 obtenida dependiendo de la implementación, y la presente invención generalmente tampoco está limitada a este respecto. En el caso de la comunicación móvil como se describe en la sección de antecedentes, particularmente la señalización RRC es adecuada para proteger por medio de la clave Ik_1.

Además, el parámetro de versión de clave v ahora se cambia del valor inicial v al siguiente valor v' de acuerdo con el esquema predeterminado, después de que se haya establecido y usado la clave modificada inicial Ik_1. Por lo tanto, v puede cambiar de 0 (cero) a 1 si se usa un esquema de incremento simple. El parámetro actualizado v 'se guarda en el terminal 300 y en el nodo 304 de control de servicio para su uso posterior en otras claves modificadas, que se explicarán a continuación. De este modo, el terminal y el nodo de control de servicio se sincronizan con respecto al parámetro v.

La siguiente figura 3B es un diagrama de señalización que ilustra una segunda fase en un procedimiento continuo de manejo de claves para la encriptación y/o integridad, siguiendo la primera fase de la figura 3A. En la figura 3B, el terminal 300 conmuta la conexión desde el primer punto 302 de servicio a un segundo punto 306 de servicio, cuando está activo. En el caso de la red móvil, esto significa que un terminal móvil hace un traspaso de una estación base a otra. Por lo tanto, el terminal está activo durante la conmutación de punto de servicio, es decir, participa en una sesión de comunicación donde se puede usar la clave Ik_1, de acuerdo con el paso 3:5 en la figura 3A como duplicado en la figura 3B.

Por alguna razón, se determina durante la sesión en curso del paso 3:5 que el terminal 300 conmutará la conexión al punto 306 de servicio. En el caso de la red móvil, los terminales móviles realizan convencionalmente mediciones de radio en señales desde estaciones base vecinas, en esta figura indicada como un paso opcional 3:6 donde el terminal 300 mide señales desde el punto 306 de servicio (o estación base). Las mediciones pueden indicar que la nueva estación base proporcionará una mejor conexión de radio que la anterior, lo que provocará un traspaso. En otros casos, puede determinarse conmutar el punto de servicio si las condiciones del servicio cambian de alguna manera, por ejemplo, cuando se activan nuevos servicios, o si se necesita más ancho de banda, o si el punto de servicio usado actualmente se ha sobrecargado o similar, etc. Incluso puede darse el caso de que el traspaso se realice en una tecnología de acceso de radio diferente, por ejemplo, de una red con celular 3G a otra con WiMAX o WLAN. Mientras las redes de radio se puedan supervisar desde la misma red central/nodo de control de servicio, la solución actual es aplicable. En ese caso, un identificador para la tecnología de acceso también puede incluirse preferiblemente como entrada para la función f tal que, por ejemplo, la nueva Ik_j = f(Ik, v, "SPj", "WLAN").

Antes de poder ejecutar la conmutación de punto de servicio, normalmente se requiere una cierta cantidad de señalización entre el terminal 300 y el antiguo punto 302 de servicio en preparación para la conmutación, como se ilustra en un paso siguiente 3:7. Esta señalización también puede protegerse con la clave Ik_1, como se indica en el paso 3:7. En el caso de la red móvil, la señalización de traspaso es generalmente una parte de la señalización RRC protegida convencionalmente por la clave básica Ik de acuerdo con los estándares actuales.

Además, el antiguo punto 302 de servicio crea una segunda clave modificada Ik_2 en este punto, como se indica en el paso 3:8, aplicando una segunda función predeterminada g al menos a la clave modificada inicial anterior Ik_1, como $Ik_2 = g(Ik_1)$. Nuevamente, pueden usarse parámetros adicionales como entrada para la función g, que sin embargo está fuera del alcance de la presente invención. Por lo tanto, la clave Ik_1 se modifica aún más en la clave Ik_2 mediante la función g.

El primer punto 302 de servicio envía la clave creada Ik_2 al segundo punto 306 de servicio en un paso siguiente 3:9. Preferiblemente, esta transmisión está protegida de alguna manera, que sin embargo está fuera del alcance de la presente invención. De acuerdo con la presente solución, la función g también es conocida por el terminal 300, que también crea la nueva clave modificada Ik_2 como se indica con un paso adicional 3:10. Cabe señalar que el paso 3:10 puede ejecutarse independientemente de los pasos 3:8 y 3:9.

Finalmente, la clave Ik_2 ahora puede ser usada por el terminal 300 y el punto 306 de servicio para proteger la comunicación durante la sesión, siempre que el terminal 300 permanezca conectado al punto 306 de servicio, como se ilustra en el paso 3:11.

Si el terminal 300 realiza más conmutaciones de punto de servicio, el procedimiento ilustrado en la figura 3B se puede repetir de modo que se use una cadena de claves modificadas, cada clave siendo calculada a partir de la

anterior usando la segunda función g: $Ik_3 = g(Ik_2)$, $Ik_4 = g(Ik_3)$, $Ik_5 = g(Ik_4)$, y así sucesivamente. La cadena completa de claves se basa originalmente en un valor del parámetro de versión de clave v, en este ejemplo el valor inicial v = 0.

De esta manera, mediante la elección adecuada de la función g, cualquier comunicación puede protegerse usando diferentes claves en diferentes puntos de servicio (por ejemplo, estaciones base) donde una clave posterior no puede revelar una anterior. También se debe tener en cuenta que si el terminal debe regresar a un punto de servicio en el que estuvo anteriormente en la misma sesión, la nueva clave será diferente de la usada anteriormente con ese punto de servicio, ya que siempre se calcula a partir de la clave anterior inmediata en la cadena.

El nodo 304 de control de servicio solo está involucrado en el establecimiento de la clave modificada inicial Ik_1 cuando el terminal entra en un modo activo al iniciar una sesión, mientras que las siguientes claves para esa sesión son manejadas únicamente por el terminal y cada nuevo punto de servicio. Esta es una operación mucho más simple en comparación con el manejo de varias claves modificadas para estaciones base vecinas de acuerdo con la propuesta de la figura 2. Además, cada nueva clave se crea de forma independiente tanto en el terminal como en el punto de servicio actual, lo que transfiere de forma segura la nueva clave al siguiente punto de servicio, suponiendo que se usan enlaces de comunicación seguros entre los puntos de servicio. Por lo tanto, no se transmite información confidencial relacionada con las claves por el aire.

La siguiente figura 3C ilustra una tercera fase en el procedimiento continuado de manejo de claves para encriptación y/o integridad, siguiendo la segunda fase de la figura 3B. Esta vez, se supone que el terminal 300 ha completado la sesión después del paso 3:11 anterior y ha entrado en modo inactivo (por ejemplo, para ahorrar batería), aunque puede permanecer registrado como presente en la red. Por ejemplo, en el caso de una red móvil, el terminal puede moverse y conectarse a varias estaciones base durante el modo inactivo, conocido como "acampar", aunque sin comunicar ningún dato. Cuando el terminal no está activo, naturalmente no se necesita ninguna clave para la protección y, por lo tanto, no se realizan operaciones de gestión de claves.

En la figura 3C, el terminal 300 está así conectado a un punto 308 de servicio llamado "x", al entrar en un modo activo al iniciar una sesión de comunicación, que se representa con el paso 3:12. Dado que el terminal ya se ha registrado con el nodo 304 de control de servicio antes en el paso 3:1 anterior, la clave básica Ik sigue siendo válida para el terminal. Para obtener una clave útil para la protección de cualquier comunicación con el terminal 300, el punto 308 de servicio ahora envía una solicitud de clave para el terminal 300 al nodo 304 de control de servicio, en un paso siguiente 3:13, que incluye una identidad de terminal. Esta solicitud de clave es típicamente parte de una "solicitud de contexto" más general para el terminal en cuestión, de acuerdo con los procedimientos convencionales.

En respuesta a esto, el nodo 304 de control de servicio recupera la clave básica Ik y nuevamente crea una clave modificada inicial Ik'_x en el paso 3:14 aplicando la primera función f predeterminada al menos a la clave básica Ik y el parámetro de versión de clave actualizada v' de tal manera que $Ik'_x = f(Ik, v')$. De este modo, la nueva clave modificada inicial Ik'_x será diferente de la calculada en el paso 3:2 anterior. Nuevamente, una identidad de punto de servicio "SPx" también puede introducirse opcionalmente en la función f para hacer que la clave Ik'_x única para esta combinación de terminal/punto de servicio, así como cualquier otro parámetro.

Cabe señalar que incluso si el terminal 300 se reactiva con el mismo punto 302 de servicio que en la figura 3A, que da como resultado una clave Ik'_1, aún sería diferente de la clave modificada inicial anterior Ik_1 debido al nuevo valor del parámetro de versión de clave v'. En un paso siguiente 3:15, el nodo 304 de control de servicio envía la nueva clave modificada inicial Ik'_x al punto 308 de servicio en respuesta a la solicitud de clave del paso 3:13.

Al mismo tiempo, es decir, independientemente de los pasos 3:13 - 3:15, el terminal 300 realiza el mismo cálculo de la clave Ik'_x basándose en el valor actualizado v', como se indica en el paso 3:16. Finalmente, la clave Ik'_x puede ahora ser usada por el terminal 300 y el punto 308 de servicio para proteger la comunicación durante la sesión, siempre que el terminal 300 permanezca conectado al punto 308 de servicio, como se ilustra en el paso 3:17.

Por lo tanto, se ha iniciado una nueva cadena de claves basada en el parámetro de versión de clave actualizado v', en este ejemplo v' = 1, que será completamente diferente de la cadena anterior. La nueva cadena continuará de la manera descrita anteriormente para la figura 3B al conmutar los puntos de servicio, siempre que el terminal permanezca activo, es decir, esté ocupado en una sesión. Cuando el terminal conmuta de un punto de servicio a otro, el antiguo y el terminal pueden eliminar su copia de la clave. Por lo tanto, solo se administra una clave a la vez.

Si el terminal permanece activo durante un período relativamente largo, lo que puede resultar en una disminución de la seguridad ya que una nueva clave se calcula con frecuencia basándose en la anterior, la seguridad se puede restaurar si se activa una nueva clave basado en un parámetro de versión de clave actualizada, incluso si el terminal no se ha reactivado desde el estado inactivo. Por ejemplo, se puede obtener una nueva clave modificada inicial si un punto de servicio actual envía una solicitud de clave al nodo 304 de control de servicio como en el paso 3:13, que puede activarse después de un período de tiempo activo preestablecido, o después de haber comunicado una cantidad predeterminada de datos, o después de un número predeterminado de conmutaciones de puntos de servicio, o de acuerdo con cualquier otro criterio especificado. La activación puede ser iniciada por el punto de

servicio actual o, alternativamente, por el terminal. El parámetro de versión de clave se restablecerá a su valor inicial después de que el terminal se haya dado de baja en la red (por ejemplo, cuando esté apagado) y se registre de nuevo, o cuando tenga lugar una nueva autenticación. Entonces se puede establecer otra clave básica Ik para el terminal.

Ahora se describirá un procedimiento básico para proporcionar claves para un terminal con referencia al diagrama de flujo ilustrado en la figura 4, tal como se ejecuta en un nodo de control de servicio en una red de comunicación que comprende una pluralidad de puntos de servicio. Dichas claves pueden usarse para proteger la comunicación entre el terminal y los puntos de servicio. Las claves y parámetros que aparecen en el ejemplo anterior de la figura 3A-C también se usan aquí.

En un primer paso 400, se establece una clave básica Ik para el terminal durante un procedimiento de registro cuando el terminal ha entrado en la red.

En un paso siguiente 402, se crea una clave modificada inicial Ik_1 aplicando una función f predeterminada al menos a la clave básica y a un valor inicial de un parámetro de versión de clave v, cuando el terminal inicia una primera sesión de comunicación.

En el siguiente paso 404, se envía la clave modificada inicial a un primer punto de servicio al que se conecta inicialmente el terminal, de modo que se pueda usar para proteger la comunicación entre el terminal y el primer punto de servicio.

En el siguiente paso 406, se recibe una solicitud de clave desde un nuevo punto de servicio (x) al que está conectado el terminal, por ejemplo, cuando el terminal entra en un estado activo después de un período en estado inactivo.

En un paso siguiente 408, se crea una nueva clave modificada inicial Ik'_x aplicando dicha función f al menos a la clave básica Ik y un valor actualizado de dicho parámetro de versión de clave v', cuando el terminal inicia una segunda sesión de comunicación.

En un paso final 410, se envía la nueva clave modificada inicial al nuevo punto de servicio, de modo que se puede usar para proteger la comunicación entre el terminal y el nuevo punto de servicio.

Ahora se describirá un procedimiento básico para obtener claves para un terminal con referencia al diagrama de flujo ilustrado en la figura 5, tal como se ejecuta en un primer punto de servicio en una red de comunicación. El terminal está inicialmente conectado al primer punto de servicio. Las claves y parámetros que aparecen en el ejemplo anterior de la figura 3A-C también se usan aquí.

En un primer paso 500, se recibe una clave modificada inicial Ik_1 desde un nodo de control de servicio, que se ha creado aplicando una primera función f predeterminada al menos a una clave básica Ik establecida para el terminal y un valor inicial de un parámetro de versión de clave v.

En un paso siguiente 502, se detecta que el terminal conmutará a un segundo punto de servicio durante una sesión en curso.

En un paso siguiente 504, se crea una segunda clave modificada Ik_2 aplicando una segunda función predeterminada g al menos a la clave modificada inicial Ik_1.

En un paso final 506, la segunda clave modificada Ik_2 se envía al segundo punto de servicio, de modo que puede usarse para proteger la comunicación entre el terminal y el segundo punto de servicio.

A continuación se describirá un procedimiento básico para obtener claves para proteger la comunicación entre un terminal y puntos de servicio en una red de comunicación con referencia al diagrama de flujo ilustrado en la figura 6, tal como se ejecuta en el terminal. El terminal está inicialmente conectado a un primer punto de servicio en la red. Las claves y parámetros que aparecen en el ejemplo anterior de la figura 3A-C también se usan aquí.

En un primer paso 600, se determina una clave básica Ik durante un procedimiento de registro al entrar en la red.

En un paso siguiente 602, se crea una clave modificada inicial Ik_1 aplicando una primera función f predeterminada al menos a la clave básica Ik y un valor inicial de un parámetro de versión de clave v, cuando se inicia una primera sesión de comunicación, de modo que se pueda usar para proteger la comunicación con el primer punto de servicio.

En un paso siguiente 604, se crea una segunda clave modificada Ik_2 aplicando una segunda función predeterminada g al menos a la clave modificada inicial Ik_1, si el terminal conmuta a un segundo punto de servicio.

En un paso siguiente 606, el terminal se conecta a un nuevo punto de servicio x después de un período de inactividad para iniciar una segunda sesión de comunicación.

En un paso final 608, se crea una nueva clave modificada inicial Ik'_x mediante la aplicación de la primera función f al menos a la clave básica Ik y un valor actualizado de dicho parámetro de versión de clave v', de modo que pueda usarse para proteger la comunicación con el nuevo punto de servicio.

El nodo de control de servicio, el punto de servicio y el terminal descritos anteriormente en relación con las figuras 4 a 6 pueden estar provistos de medios adecuados para ejecutar los pasos descritos en los diagramas de flujo mostrados en la figura 4, la figura 5 y la figura 6, respectivamente.

Al usar la presente solución, por ejemplo, de acuerdo con cualquiera de las realizaciones descritas, se obtiene un mecanismo simple pero seguro para manejar claves para proteger la comunicación entre terminales y puntos de servicio en una red de comunicación. Las nuevas claves se establecen de forma segura cada vez que el terminal conmuta el punto de servicio, y no se requieren predicciones de traspaso. El número de claves que deben manejar las estaciones base u otros puntos de servicio también se mantiene al mínimo. La seguridad hacia atrás confiable al conmutar los puntos de servicio, y la seguridad hacia adelante cuando un terminal inicia una sesión, también se puede obtener con un impacto mínimo de servicio.

Aunque las realizaciones descritas anteriormente se han dirigido principalmente al caso de una red móvil, la presente invención se puede implementar en varios tipos diferentes de redes de comunicación. Por ejemplo, la invención también se puede implementar en WiMAX/802.16, WLAN/802.11 y Flarion/802.20 (o 802.21).

Si bien la invención se ha descrito con referencia a realizaciones de ejemplo específicas, la descripción solo pretende ilustrar el concepto inventivo y no debe considerarse como limitativa del alcance de la invención. Se pueden usar diversas alternativas, modificaciones y equivalentes sin apartarse de la invención, que se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1.- Un método, como se ejecuta en un nodo de control de servicio en una red de comunicación que comprende una pluralidad de puntos de servicio, de proporcionar claves para proteger la comunicación entre un terminal y dichos puntos de servicio, que comprende los siguientes pasos:

- A) establecer (600; 3:1) una clave básica (Ik) para el terminal durante un procedimiento de registro cuando el terminal ha entrado en la red, e inicializar un parámetro de versión de clave (v) en un valor inicial;

- B) crear (602; 3:2) una clave modificada inicial (Ik_1) aplicando una función predeterminada (f) al menos a la clave básica y al valor inicial del parámetro de versión de clave (v), cuando el terminal inicia una primera sesión de comunicación;

- C) enviar (3:3) la clave modificada inicial a un punto de servicio al cual el terminal está inicialmente conectado, siendo utilizable la clave modificada para proteger la comunicación entre el terminal y el punto de servicio;

- D) recibir (3:13) una solicitud de clave desde un nuevo punto de servicio; y

- E) actualizar (3:14) dicho valor de dicho parámetro de versión de clave (v), a un valor actualizado (v') cambiándolo de acuerdo con un esquema o algoritmo predeterminado, y crear una segunda clave modificada inicial (Ik'_x) basándose en la clave básica (Ik) y dicho parámetro actualizado de versión de clave (v').

2.- Un método de acuerdo con la reivindicación 1, que comprende el siguiente paso adicional:

- F) enviar (3:15) la segunda clave modificada inicial al nuevo punto de servicio, de modo que puede usarse para proteger la comunicación entre el terminal y el nuevo punto de servicio.

3.- Un método de acuerdo con la reivindicación 1 o 2, en el que una identidad de punto de servicio ("SP1", "SPx") también se introduce en la función predeterminada al crear una clave modificada inicial y/o una nueva clave modificada inicial, para hacer la clave única para la combinación particular de terminal/punto de servicio.

4.- Un método de acuerdo con cualquiera de las reivindicaciones 1 a 3, en el que el valor del parámetro de versión de clave (v) se inicializa a un cierto valor y luego se cambia de acuerdo con un esquema o algoritmo predeterminado cada vez que se crea una nueva clave modificada inicial.

5.- Un método de acuerdo con la reivindicación 4, en el que el parámetro de versión de clave se inicializa a cero y luego se incrementa en uno cada vez que se crea una nueva clave modificada inicial.

6.- Un método de acuerdo con cualquiera de las reivindicaciones 2 a 5, en el que se recibe la solicitud de clave cuando el terminal se reactiva después de estar inactivo.

7.- Un método de acuerdo con cualquiera de las reivindicaciones 2 a 5, en el que se recibe la solicitud de clave después de que el terminal ha estado activo un período de tiempo preestablecido, o ha comunicado una cantidad predeterminada de datos, o ha realizado un número predeterminado de conmutaciones de puntos de servicio.

8.- Una disposición en un nodo de control de servicio en una red de comunicación que comprende una pluralidad de puntos de servicio, para proporcionar claves para proteger la comunicación entre un terminal y dichos puntos de servicio, estando configurada la disposición para:

- establecer una clave básica (Ik) para el terminal durante un procedimiento de registro cuando el terminal ha entrado en la red, e inicializar un parámetro de versión de clave (v) en un valor inicial;

- crear una clave modificada inicial (Ik_1) aplicando una función predeterminada (f) al menos a la clave básica y a un valor inicial de un parámetro de versión de clave (v), cuando el terminal inicia una primera sesión de comunicación;

- enviar la clave modificada inicial a un primer punto de servicio al que está conectado inicialmente el terminal, de modo que pueda usarse para proteger la comunicación entre el terminal y el primer punto de servicio;

- recibir una solicitud de clave desde un nuevo punto de servicio, y

- actualizar dicho valor de dicho parámetro de versión de clave (v), a un valor actualizado (v') cambiándolo de acuerdo con un esquema o algoritmo predeterminado, y

- crear una segunda clave modificada inicial (Ik'_x) basándose en la clave básica (Ik) y dicho parámetro de versión de clave (v') actualizado.

9.- Una disposición de acuerdo con la reivindicación 8, estando configurada la disposición además para:

- enviar la segunda clave modificada inicial al nuevo punto de servicio, de modo que puede usarse para proteger la comunicación entre el terminal y el nuevo punto de servicio.

10.- Una disposición de acuerdo con la reivindicación 8 o 9, configurada además para crear una clave modificada inicial y/o una nueva clave modificada inicial y también para introducir una identidad de punto de servicio ("SP1", "SPx") a la función predeterminada al crear la clave modificada inicial y/o nueva clave modificada inicial, para hacer la clave única para la combinación particular de terminal/punto de servicio.

11.- Una disposición de acuerdo con cualquiera de las reivindicaciones 8 a 10, configurada además para inicializar el valor del parámetro de versión de clave (v) a un cierto valor y luego cambiarlo de acuerdo con un esquema o algoritmo predeterminado cada vez que se crea una nueva clave modificada inicial.

12.- Una disposición de acuerdo con la reivindicación 11, configurada además para inicializar el parámetro de versión de clave a cero y luego incrementarlo en uno cada vez que se crea una nueva clave modificada inicial.

13.- Un método, como se ejecuta en un terminal conectado inicialmente a un primer punto de servicio en una red de comunicación, para obtener claves para proteger la comunicación con los puntos de servicio en la red, que comprende los siguientes pasos:

- A) determinar (400; 3:1) una clave básica (Ik) durante un procedimiento de registro al entrar a la red, e inicializar un parámetro de versión de clave (v) en un valor inicial;

- B) crear (402; 3:4) una clave modificada inicial (Ik_1) aplicando una primera función predeterminada (f) a al menos la clave básica y al valor inicial de un parámetro de versión de clave (v), al iniciar una primera sesión de comunicación, de modo que puede usarse para proteger la comunicación con el primer punto de servicio;

- C) conectarse a un nuevo punto de servicio;

- D) actualizar (408; 3:16) dicho valor de dicho parámetro de versión de clave (v) a un valor actualizado (v') de acuerdo con un esquema o algoritmo predeterminado; y

- E) crear (408; 3:10) una segunda clave modificada (Ik_2) basándose en la clave básica (Ik) y dicho parámetro de versión de clave (v') actualizado.

14.- Un método de acuerdo con la reivindicación 13, en el que una identidad de punto de servicio ("SP1", "SPx") también se introduce en la función predeterminada al crear la clave modificada inicial y/o la nueva clave modificada inicial, para hacer la clave única para la combinación particular de terminal/punto de servicio.

15.- Un método de acuerdo con cualquiera de las reivindicaciones 13 a 14, en el que el valor del parámetro de versión de clave (v) se inicializa a un cierto valor y luego se cambia de acuerdo con un esquema o algoritmo predeterminado cada vez que se crea una nueva clave modificada inicial.

16.- Un método de acuerdo con la reivindicación 15, en el que el parámetro de versión de clave se inicializa a cero y luego se incrementa en uno cada vez que se crea una nueva clave modificada inicial.

17.- Una disposición en un terminal inicialmente conectado a un primer punto de servicio en una red de comunicación, para obtener claves para proteger la comunicación con puntos de servicio en la red, estando configurada la disposición para:

- determinar una clave básica (Ik) durante un procedimiento de registro al entrar en la red, e inicializar un parámetro de versión de clave (v) en un valor inicial;

- crear una clave modificada inicial (Ik_1) aplicando una primera función predeterminada (f) al menos a la clave básica y al valor inicial de un parámetro de versión de clave (v), al iniciar una primera sesión de comunicación, de modo que puede usarse para proteger la comunicación con el primer punto de servicio;

- conectarse a un nuevo punto de servicio, y

- actualizar dicho valor de dicho parámetro de versión de clave (v), a un valor actualizado (v') cambiándolo de acuerdo con un esquema o algoritmo predeterminado y crear una segunda clave modificada inicial (Ik_2) basándose en la clave básica (Ik) y dicho parámetro de versión de clave (v') actualizado.

18.- Una disposición de acuerdo con la reivindicación 17, en la que dicha disposición está configurada además para:

- conectarse a un nuevo punto de servicio (x) después de un período inactivo para iniciar una segunda sesión de comunicación.

19.- Una disposición de acuerdo con la reivindicación 17 o 18, configurada además para crear una clave modificada inicial y/o una nueva clave modificada inicial y también para introducir una identidad de punto de servicio ("SP1", "SPx") a la función predeterminada al crear la clave modificada inicial y/o la nueva clave modificada inicial, para hacer la clave única para la combinación particular de terminal/punto de servicio.

20.- Una disposición de acuerdo con cualquiera de las reivindicaciones 17 a 19, configurada además para inicializar el valor del parámetro de versión de clave (v) a un cierto valor y luego cambiarlo de acuerdo con un esquema o algoritmo predeterminado cada vez que se crea una nueva clave modificada inicial.

21.- Una disposición de acuerdo con la reivindicación 20, configurada además para inicializar el parámetro de versión de clave a cero y luego incrementarlo en uno cada vez que se crea una nueva clave modificada inicial.

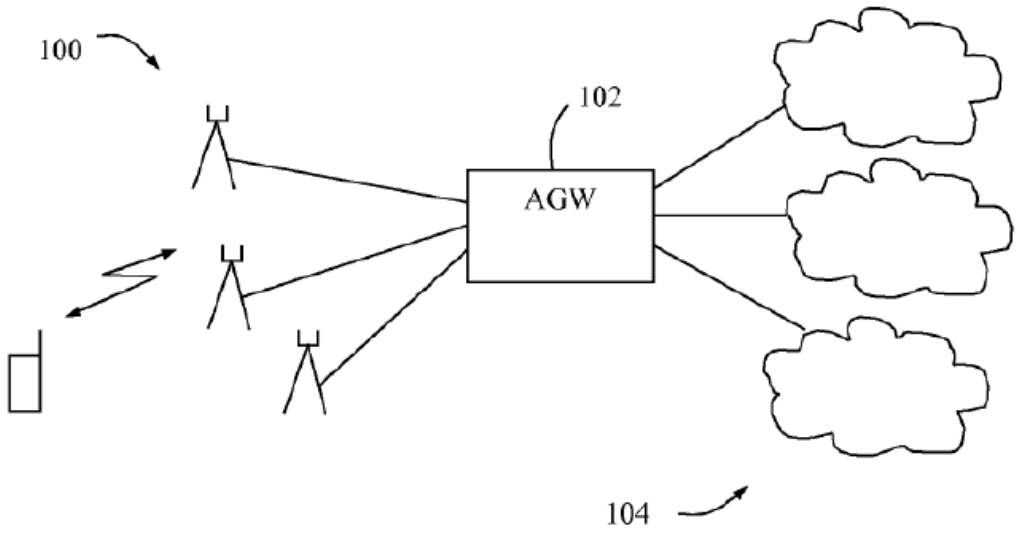

Fig. 1 (Técnica anterior)

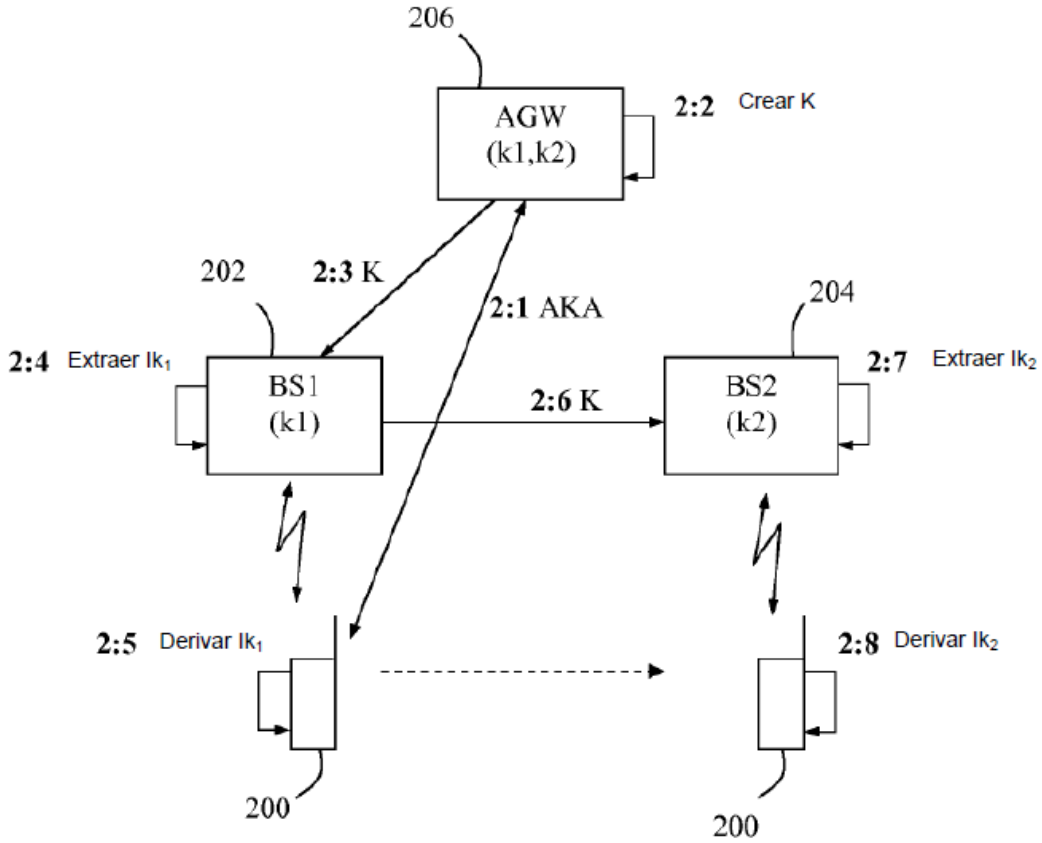

Fig. 2 (Técnica anterior)

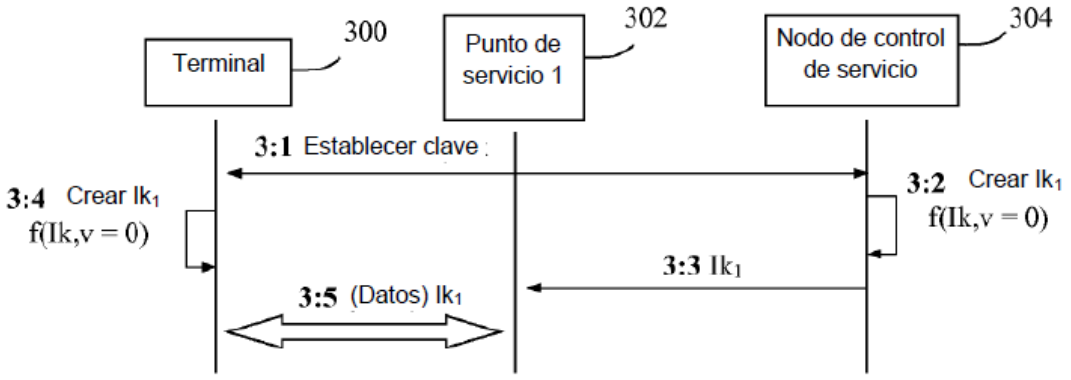

Fig. 3A

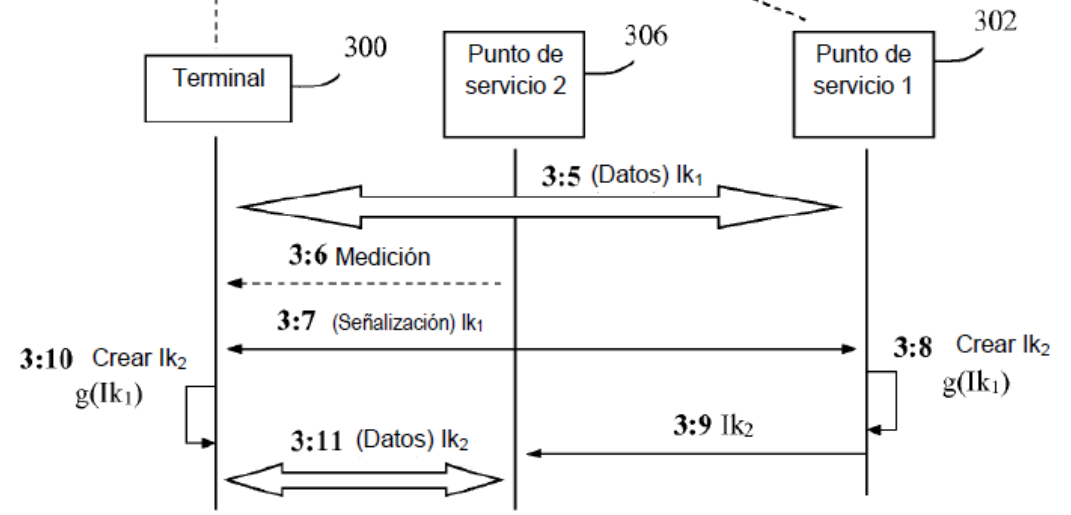

Fig. 3B

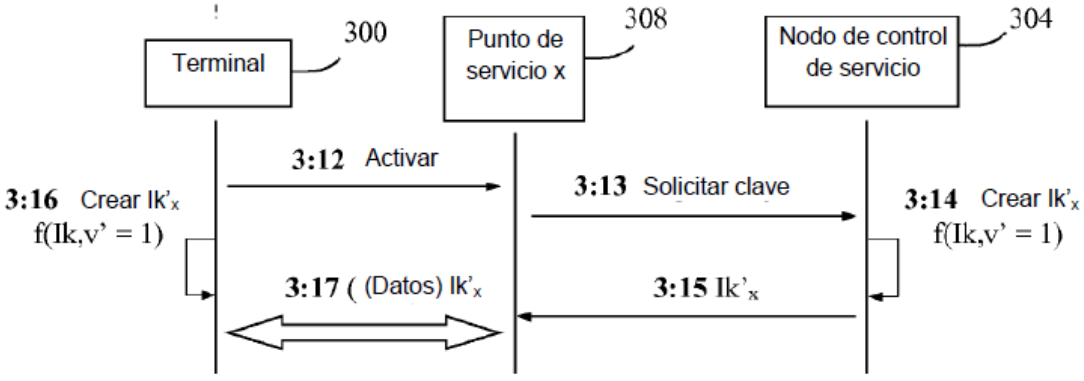

Fig. 3C

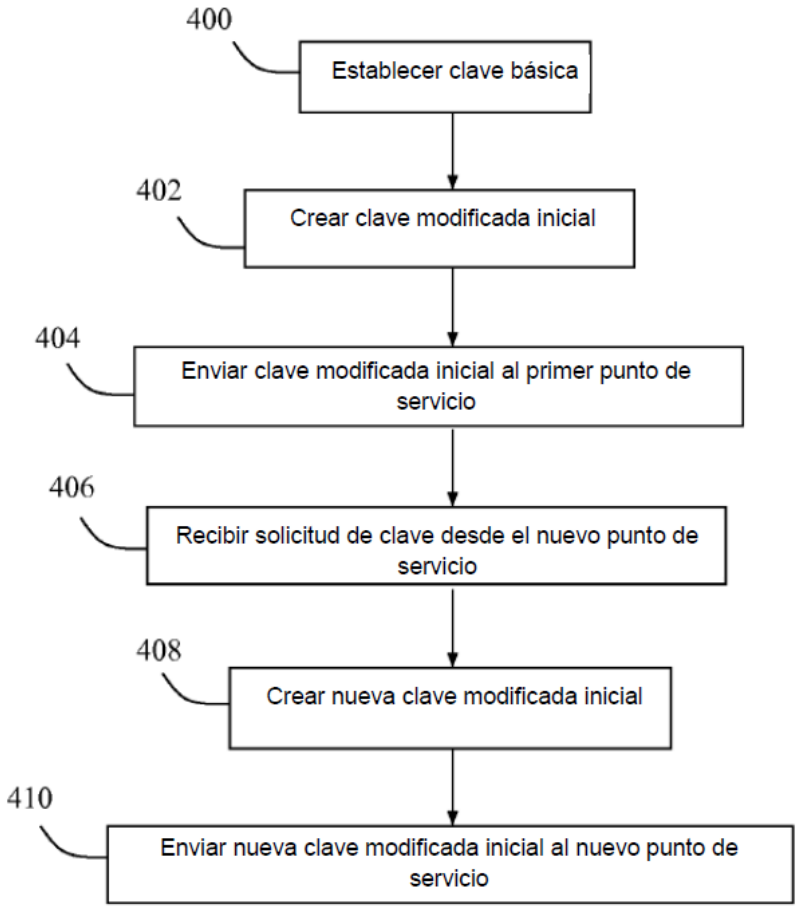
400
Establecer clave básica
402
Crear clave modificada inicial
404
Enviar clave modificada inicial al primer punto de servicio
406
Recibir solicitud de clave desde el nuevo punto de servicio
408
Crear nueva clave modificada inicial
410
Enviar nueva clave modificada inicial al nuevo punto de servicio

Fig. 4

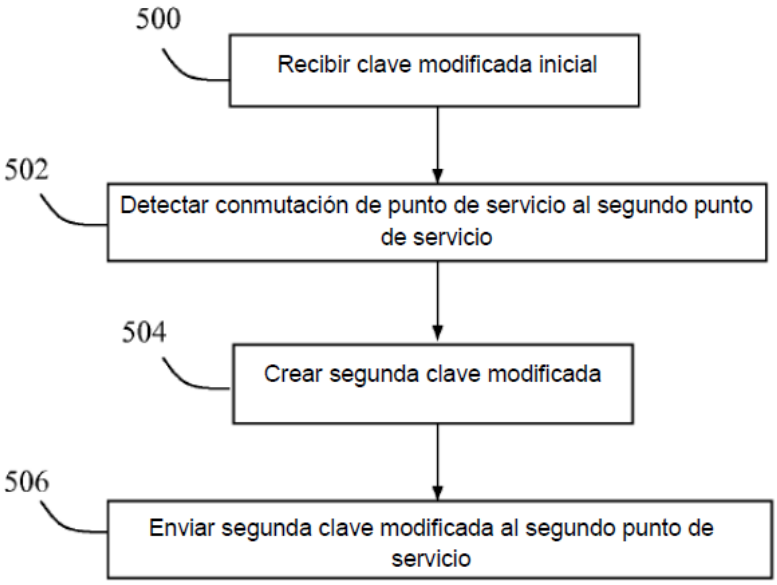
500
Recibir clave modificada inicial
502
Detectar conmutación de punto de servicio al segundo punto de servicio
504
Crear segunda clave modificada
506
Enviar segunda clave modificada al segundo punto de servicio

Fig. 5

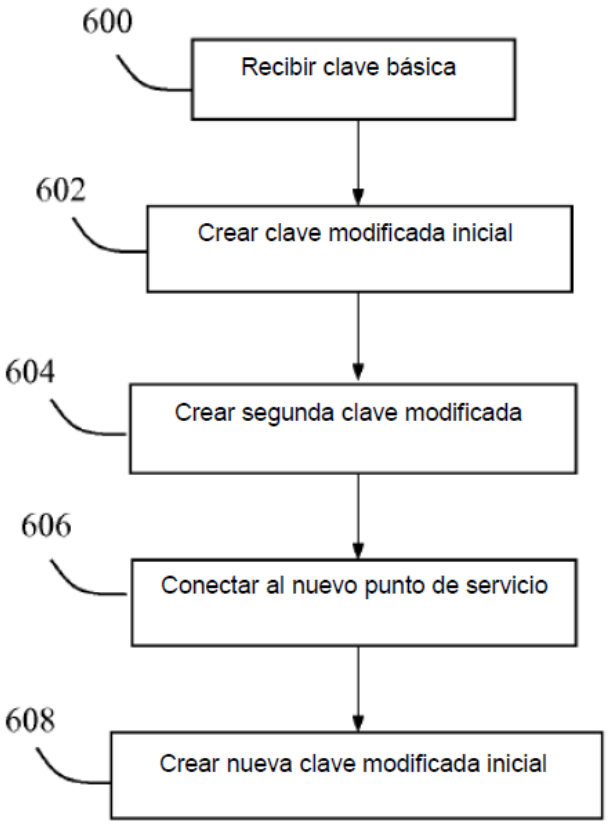
600
Recibir clave básica
602
Crear clave modificada inicial
604
Crear segunda clave modificada
606
Conectar al nuevo punto de servicio
608
Crear nueva clave modificada inicial

Fig. 6