(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 625 133**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.03.2007 PCT/SE2007/000287**

(87) Fecha y número de publicación internacional: **04.10.2007 WO07111557**

(96) Fecha de presentación y número de la solicitud europea: **23.03.2007 E 07747962 (4)**

(97) Fecha y número de publicación de la concesión europea: **22.02.2017 EP 1999930**

(54) Título: **Un método y aparato para manejar claves utilizadas para cifrado 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:
18.07.2017

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
SVARDVAGEN 2
S-175 68 JARFALLA, SE

(72) Inventor/es:

BLOM, ROLF;
NORRMAN, KARL y
NÄSLUND, MATS

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Un método y aparato para manejar claves utilizadas para cifrado 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 los puntos de servicio en una red de comunicación.

Antecedentes

En la comunicación inalámbrica, la seguridad es un tema importante, ya que transmitir información por aire permite interceptar y/o modificar ilícitamente la información comunicada. Por lo tanto, la información normalmente es cifrada y/o protegida por integridad antes de ser enviada por aire. Los estándares de comunicación predominantes de hoy 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 paquetes de radio) y UMTS (sistema universal de telecomunicaciones móviles) utilizan dos claves denominadas Ck e Ik, para asegurar la integridad y para cifrar información comunicada a través de 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 se puede utilizar para cifrar 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 a utilizar en una sesión se establecen durante una etapa de registro cuando el terminal se conecta a la red, que se denominará acuerdo clave en esta descripción. Debe tenerse en cuenta que un terminal móvil puede estar en dos modos diferentes denominados modo inactivo cuando se ha registrado como presente en la red pero no está implicado 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 denominados datos de "plano de usuario", 2) señalización de NAS (estrato sin acceso) que es información relacionada, por ejemplo, con la seguridad que incluye autentificación y cifrado, y 3) RRC (control de recursos de radio), que es información relacionada con la comunicación por radio, incluidos los esquemas de modulación y multiplexación específicos de canal, la regulación de potencia, las mediciones de señal, etc.

En los llamados sistemas 3G de acuerdo con UMTS, los datos del plano de usuario son transportados normalmente en cuatro nodos diferentes en la red de acceso: la estación base (también denominada 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), de los cuales las estaciones base y RNC constituyen una parte de red de radio y el SGSN y GGSN constituyen una parte de red de núcleo. En los sistemas 3G, todo el cifrado/descifrado de datos del plano de usuario, NAS y RRC es ejecutado por el RNC y el terminal, mientras que en los sistemas GSM tradicionales, el cifrado es manejado 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 asociación de tercera generación). La nueva arquitectura comprende básicamente dos tipos de nodos que incluyen estaciones base "evolucionadas" 100 en la parte de red de radio conectada a una pasarela de control de acceso central AGW 102 en la parte de red de núcleo por medio de la conocida interfaz S1. Una red de acceso puede contener varios nodos AGW que sirven diferentes áreas geográficas. El nodo AGW está conectado a diferentes redes externas 104 que utilizan interfaces bien conocidas, incluyendo Internet (que utiliza la interfaz Gi), otras redes 3GPP (que utilizan la interfaz Gn) y redes no 3GPP (que utilizan la interfaz S2), e incluye ciertas funciones similares a las actualmente implementadas en el RNC, SGSN y GGSN.

En particular, el procesamiento de seguridad relacionado con el cifrado y la integridad tendrá lugar en la estación base 100 y el nodo AGW 102. Básicamente, el cifrado de datos de plano de usuario, y potencialmente también la señalización de NAS, serán manejados por el nodo AGW 102, mientras que la protección de la señalización de RRC será manejada por las estaciones base 100. El proceso inicial de autenticación del acuerdo de abonado y clave se llevará a cabo entre un SIM (módulo de identidad de suscriptor) en el terminal y el nodo AGW, y se denomina a menudo AKA (acuerdo de autentificación y clave). De este modo, las claves Ck e Ik antes mencionadas pueden ser establecidas por el terminal y el nodo AGW durante el proceso AKA.

Con el fin de proporcionar interoperabilidad entre diferentes arquitecturas de red, es altamente deseable que los componentes de seguridad y las rutinas de los sistemas 3G existentes puedan ser reutilizados en la arquitectura de dos nodos antes descrita, incluyendo 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, preferentemente basándose en las claves Ck e Ik anteriores. 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 utilizar 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 por estar situada normalmente en lugares de fácil acceso y sin vigilancia, en comparación con el nodo AGW más centralizado que se puede instalar completamente protegido. Por lo tanto, existe el riesgo de que la clave Ik sea interceptada en la estación base de tal manera que la señalización NAS pueda detectarse ilícitamente. Debe observarse en este contexto que la información sensible del NAS generalmente demanda un mayor grado de seguridad que la información del CRR. 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 en que la información interceptada se registra y se reproduce más tarde (denominados ataques de repetición), si se utiliza la misma clave para dos propósitos diferentes que proporciona oportunidades múltiples para detectar la clave utilizada. Por lo tanto, si Ik se reutiliza en la estación base, se requiere que el nodo AGW aplique al menos una función unidireccional f a Ik antes de enviarla en una forma así modificada f (Ik) = Ik' a la estación base.

Sin embargo, si Ik' se intercepta en una estación base durante una sesión, este error de seguridad persistirá incluso si la sesión es transferida a una nueva estación base, es decir, mientras se use Ik'. Este problema se puede evitar si el proceso AKA se repite a intervalos regulares (por ejemplo, se desencadena mediante transferencia), lo que sin embargo puede perturbar la sesión, repercutiendo de este modo significativamente en un comportamiento sin interrupciones deseable de los servicios.

Por lo tanto, es deseable evitar la inseguridad persistente que sigue a una interceptación de claves cuando el terminal se desplaza entre diferentes puntos de servicio, es decir, estaciones base, sin requerir operaciones adicionales tales como el establecimiento de nuevas claves en una reautentificación de acuerdo con el proceso AKA. Se ha realizado un intento de cumplir estos objetivos implicando un nuevo tipo de clave que se comparte entre la estación base y el nodo AGW, de acuerdo con un procedimiento propuesto descrito 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 central AGW 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 así las claves predefinidas k1 yk2, respectivamente, con el nodo AGW 206.

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

Con el fin de establecer una protección adicional, el nodo AGW 206 buscará entonces la clave k1 de BS1. Además, el nodo AGW buscará también la clave correspondiente de un número adecuado de estaciones base "vecinas", es decir, estaciones base situadas cerca de la estación base de servicio BS1 a la cual el terminal podría ser transferido cuando se mueve durante una sesión, incluyendo BS2 204. Las estaciones base vecinas deben ser seleccionadas como cubriendo un área razonable en la cual se espera que el terminal esté. Alrededor de 5-10 estaciones base pueden considerarse como estaciones base vecinas, por ejemplo dependiendo del tamaño de sus células.

A continuación, el nodo AGW 206 utiliza la clave Ik establecida para el terminal 200, para crear una clave modificada específicamente para cada estación base, aplicando una función predeterminada f 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. Debe observarse que la función predeterminada f también es conocida por el terminal, que se utilizará como se describe a continuación.

Cada clave Ik modificada producida Ik_1, Ik_2... Ik_j es entonces "envuelta" (es decir, cifrada) por la clave k compartida con la estación base correspondiente, componiendo en total 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). En lo que sigue, "K" se utilizará para representar brevemente el conjunto completo de todas estas claves envueltas. Todo el proceso de creación de K como se ha descrito anteriormente se ilustra mediante un paso 2:2 en la figura.

De acuerdo con el procedimiento propuesto, el nodo AGW 206 transfiere ahora todo el conjunto de claves K a la estación base de servicio BS1 202, en el siguiente paso 2:3. BS1 puede entonces descifrar el componente de K correspondiente a Encr (k1, Ik_1) utilizando su clave única k1, para extraer la clave Ik modificada anteriormente mencionada Ik1 originalmente creada para esa estación base, en un siguiente paso 2:4, para ser compartido con el terminal. BS1 también almacena todo el conjunto de claves K para uso futuro.

Dado que el terminal conoce naturalmente su clave Ik original y la identidad de la estación base de servicio "BS1",

puede derivar la misma clave Ik modificada Ik_1 aplicando la función f: Ik_1 = f (Ik, "BS1"), en relación 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 Ik_1 puede ahora ser utilizada por el terminal 200 y la estación base 202 para proteger la señalización RRC durante la sesión, mientras el terminal 200 permanezca conectado a la estación base 202.

Si el terminal en algún momento durante la sesión se mueve para ser transferido a una nueva estación base, en este caso BS2 204 como se ilustra mediante la flecha discontinua, la antigua BS1 202 transfiere todo el conjunto de claves K a BS2 204, en un paso 2:6. Utilizando el conjunto de claves K recibido, la BS2 204 puede extraer de manera similar su propia clave Ik modificada Ik_2 en un paso 2:7. El terminal también derivará Ik_2 utilizando la función f (Ik, "BS2"), en un paso 2:8, para ser utilizado como clave para el cifrado y/o la integridad en comunicación adicional.

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

Por lo tanto, la solución de la técnica anterior descrita anteriormente proporciona claves únicas para cada combinación estación base-terminal. Incluso si en algún momento una clave Ik_x utilizada en una célula x (es decir, estación base) es interceptada ilícitamente, se utilizará una nueva clave Ik_y en cuanto se produce una transferencia a otra célula y, y el error de seguridad no persiste. Por lo tanto, la solución en la figura 2 proporciona seguridad hacia atrás y hacia adelante siempre que se cambie la estación base de servicio.

Sin embargo, hay algunos problemas significativos 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 solamente se utilizarán algunas, si las hubiere. Además, el nodo AGW tiene que "predecir" qué estaciones base posiblemente podrían estar involucradas en futuras transmisiones, 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 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, las estaciones base de servicio están obligadas a almacenar todo el conjunto de claves K, y no solamente su "propia" clave, y transferirla a la siguiente estación base después de la transferencia.

En general, es deseable obtener una manera sencilla pero fiable de utilizar claves para la protección de cifrado y/o integridad, particularmente cuando un terminal de comunicación cambia la comunicación desde un punto de servicio a otro punto de servicio. Más específicamente, sería beneficioso evitar la necesidad de predicciones de transferencia y reducir el número de claves que deben ser manejadas por las estaciones base u otros puntos de servicio. También es deseable proporcionar seguridad hacia atrás al cambiar puntos de servicio, y seguridad hacia delante cuando un terminal inicia una sesión, por ejemplo, pasa del modo inactivo al modo activo, con un impacto mínimo en el servicio.

Aunque la descripción de antecedentes anterior se ha centrado en terminales móviles que utilizan estaciones base en una red 3G como puntos de servicio, las cuestiones discutidas pueden ser relevantes para otras redes de acceso móviles (o celulares), y también para redes de acceso fijo que utilizan conexiones cableadas tales como DSL (línea de abonado digital), PON (red óptica pasiva) y DOCSIS (datos sobre la especificación de interfaz de servicio de cable). Por ejemplo, el proceso AKA anteriormente mencionado puede ser reemplazado por otros procesos similares para establecer una o más claves que se utilizarán en las comunicaciones de sesión, dependiendo de las rutinas de red predominantes. Además, al ver "acceso" o "conectividad" como 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 dirigirse generalmente a los problemas y demandas esbozados anteriormente y proporcionar un mecanismo conveniente para obtener claves para proteger la comunicación entre un terminal y los puntos de servicio en una red de comunicación.

Este objeto y otros se pueden obtener 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 los puntos de servicio en una red de comunicación, tal como se implementa en un nodo de control de servicio. Se establece primero una clave básica para el terminal durante un procedimiento de registro cuando el terminal ha entrado en la red. Una clave modificada inicial se crea entonces aplicando una función predeterminada a al menos la clave básica y 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

está conectado inicialmente el terminal, de manera que puede utilizarse 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 estado activo después de un período en estado inactivo. En respuesta a ello, se crea una nueva clave modificada inicial aplicando dicha función a al menos la clave básica y 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 puede utilizarse para proteger la comunicación entre el terminal y el nuevo punto de servicio.

Una identidad de punto de servicio también se puede introducir en 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 de terminal/punto de servicio particular.

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 se puede inicializar a cero y luego se incrementa en uno cada vez que se crea una nueva clave modificada inicial.

La solicitud de clave puede ser recibida cuando el terminal es reactivado después de estar inactivo, o después de que el terminal ha estado activo durante un período de tiempo preestablecido, o ha comunicado una cantidad predeterminada de datos, o ha hecho un número predeterminado de cambios 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, primero se recibe una clave modificada inicial desde un nodo de control de servicio, que se ha creado aplicando una primera función predeterminada a al menos una clave básica establecida para el terminal y un valor inicial de un parámetro de versión de clave. Cuando se detecta que el terminal cambiará a un segundo punto de servicio durante una sesión en curso, se crea una segunda clave modificada aplicando una segunda función predeterminada a al menos la clave modificada inicial. La segunda clave modificada se envía finalmente al segundo punto de servicio, de modo que puede ser utilizada 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 ser enviada cuando el terminal se reactiva después de estar inactivo, o después de que el terminal ha estado activo durante un período de tiempo preestablecido, o ha comunicado una cantidad predeterminada de datos o ha hecho un número predeterminado de cambios de punto de servicio.

Se definen adicionalmente un método y una disposición para obtener claves para proteger la comunicación con puntos de servicio en una red de comunicación, tal como se ejecutan en un terminal inicialmente conectado a un primer punto de servicio en la red. Una clave básica Ik se determina primero durante un procedimiento de registro al entrar en la red. Una clave modificada inicial se crea entonces aplicando una primera función predeterminada a al menos la clave básica y un valor inicial de un parámetro de versión de clave, al iniciar una primera sesión de comunicación, de tal manera que se puede utilizar para proteger la comunicación con el primer punto de servicio. Si el terminal cambia entonces a un segundo punto de servicio, se crea una segunda clave modificada aplicando una segunda función predeterminada a al menos la clave modificada inicial.

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

Una identidad de punto de servicio también se puede introducir en 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 de terminal/punto de servicio particular.

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 se puede inicializar a cero y luego se incrementa 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 que se acompañan, 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 puede utilizarse la presente invención.

- La figura 2 es un diagrama de bloques esquemático que ilustra un procedimiento propuesto de manejo de 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 desde la figura 3A.

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

- La figura 4 es un diagrama de flujo que ilustra un procedimiento básico de 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 de obtención de 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 de obtención de 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 en primer lugar 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 cifrado y/o integridad en una red de acceso a comunicaciones, por ejemplo, la red de acceso móvil mostrada 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 un AGW, como se ha descrito anteriormente. En esta descripción, el término "nodo de control de servicio" puede representar en general cualquier nodo de red central, por ejemplo en una red de núcleo, que controla 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 el cifrado y/o la 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 une inicialmente a una estación base, es decir, el punto 302 de servicio. Esta clave básica se denomina aquí Ik en analogía con el procedimiento propuesto de la figura 2, aunque otras claves como Ck también se pueden utilizar en la presente solución. Además, la presente solución se puede aplicar para cualquier número de claves que se pueden emplear para diferentes propósitos, tales como cifrado, integridad, autenticación, etc., pero para simplificar solamente se describirá en esta realización una clave Ik.

Como se ilustra en el siguiente paso 3:2, el nodo 304 de control de servicio crea una clave modificada inicial Ik_1 aplicando una primera función predeterminada f a al menos la clave original Ik y opcionalmente también una identidad de punto de servicio "SP1" para hacer que la clave Ik_1 única para esta combinación de terminal/punto de servicio, similar a la creación de claves modificadas en la propuesta de la figura 2. Otros parámetros también pueden utilizarse aquí como entrada a la función f, tales como otras claves básicas (por ejemplo, Ck) y una identidad terminal, que está sin embargo 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 manera que $Ik_1 = f(Ik, v)$. Como se ha mencionado anteriormente, "SP1" y/u otros parámetros también pueden utilizarse como entrada para la función f. El valor del parámetro de versión de clave v se cambiará de acuerdo con un esquema predeterminado cada vez que se cree una clave modificada Ik_1 como se describe a continuación, indicada aquí como v, v ‘, v’’, v’’’, etc. Por ejemplo, el parámetro de versión de clave v puede inicializarse a v = 0 (cero) y luego simplemente incrementarse por uno de manera que v '= 1, v "= 2, v"' = 3, etc., que se utiliza en la presente realización. Sin embargo, el valor del parámetro de versión de clave v puede cambiarse de acuerdo con cualquier esquema o algoritmo concebible, y la presente solución no está limitada a este respecto. Debe observarse que el valor actual del parámetro v y la función f deberían 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 siguiente paso 3:3, para su uso 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 mediante un paso 3:4. Debe observarse 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 puede ahora ser utilizada por el terminal 300 y el punto 302 de servicio para proteger cualquier comunicación durante la sesión, mientras el terminal 300 permanezca conectado al punto 302 de servicio, que se ilustra mediante un paso 3:5. En este paso, "(Datos) Ik_1" generalmente indica que los datos comunicados están protegidos por Ik_1.

En términos generales, cualquier tipo de comunicación puede ser protegida de cualquier manera mediante la clave Ik_1 obtenida dependiendo de la implementación, y la presente invención tampoco está generalmente 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 mediante la clave Ik_1.

Además, el parámetro de versión de clave v se cambia ahora del valor inicial v al siguiente valor v' de acuerdo con el esquema predeterminado, después de que se ha establecido y utilizado la clave modificada inicial Ik_1. Así, v puede cambiar de 0 (cero) a 1 si se utiliza un esquema de incremento simple. El parámetro actualizado v' se guarda entonces tanto en el terminal 300 como en el nodo 304 de control de servicio para uso posterior en otras claves modificadas, que se explicarán a continuación. De este modo, el terminal y el nodo de control de servicio están sincronizados 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 cifrado y/o integridad, después de la primera fase de la figura 3A. En la figura 3B, el terminal 300 cambia 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 realiza una transferencia de una estación base a otra. De este modo, el terminal está activo durante el cambio de punto de servicio, es decir, aplicado en una sesión de comunicación en la que se puede utilizar la clave Ik_1, de acuerdo con el paso 3:5 en la figura 3A como se duplica en la figura 3B.

Por la razón que sea, se determina así durante la sesión en curso del paso 3:5 que el terminal 300 cambiará la conexión al punto 306 de servicio. En el caso de la red móvil, los terminales móviles realizan convencionalmente mediciones de radio sobre señales de estaciones base vecinas, en esta figura se indica como un paso opcional 3:6 donde el terminal 300 mide señales desde el punto de servicio (o estación base) 306. Las mediciones pueden entonces indicar que la nueva estación base proporcionará una mejor conexión de radio que la antigua, provocando de este modo una transferencia. En otros casos, se puede determinar cambiar el punto de servicio si las condiciones de servicio de alguna manera cambian, por ejemplo, cuando se activan nuevos servicios, o si se necesita más ancho de banda, o si el punto de servicio actualmente utilizado se ha sobrecargado o similar, etc. Puede incluso ser el caso de que la transferencia se realice a una tecnología de acceso de radio diferente, por ejemplo desde una red que utiliza un teléfono celular 3G a otro que utiliza WiMAX o WLAN. Siempre y cuando las redes de radio puedan ser supervisadas desde el mismo nodo central de control de red/servicio, la presente solución es aplicable. En este caso, también se puede incluir preferentemente un identificador para la tecnología de acceso como entrada a la función f de manera que, por ejemplo, el nuevo Ik j = f (Ik, v, "SPj", "WLAN").

Antes de que se pueda ejecutar el cambio 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 el cambio, como se ilustra en el siguiente paso 3:7. Esta señalización puede ser protegida también por la clave Ik_1, como se indica en el paso 3:7. En el caso de la red móvil, la señalización de transferencia es generalmente una parte de la señalización RRC protegida convencionalmente por la clave básica Ik de acuerdo con los estándares actuales.

Además, el punto 302 de servicio antiguo crea una segunda clave modificada Ik_2 en este punto, como se indica mediante un paso 3:8, aplicando una segunda función predeterminada g a al menos la clave modificada inicial Ik_1 de manera que $Ik_2 = g(Ik_1)$. De nuevo, se pueden utilizar otros parámetros 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 adicionalmente en la clave Ik_2 por medio de la función g.

El primer punto 302 de servicio envía entonces la clave creada Ik_2 al segundo punto 306 de servicio en un paso siguiente 3:9. Preferentemente, 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 por un paso adicional 3:10. Debe tenerse en cuenta que el paso 3:10 puede ejecutarse independientemente de los pasos 3:8 y 3:9.

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

Si el terminal 300 realiza otros cambios de punto de servicio, el procedimiento ilustrado en la figura 3B puede

repetirse de tal manera que se utilice una cadena de claves modificadas, calculándose cada clave a partir de la anterior utilizando la segunda función g: $Ik_3 = g(Ik_2)$, $Ik_4 = g(Ik_3)$, $Ik_5 = g(Ik_4)$, y así sucesivamente. Toda la cadena 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 ser protegida utilizando diferentes claves en diferentes puntos de servicio (por ejemplo, estaciones base) donde una clave posterior no puede revelar una anterior. También debe tenerse en cuenta que si el terminal debe volver a un punto de servicio en el que ha estado anteriormente en la misma sesión, la nueva clave será diferente de la utilizada 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 solamente participa en el establecimiento de la clave modificada inicial Ik_1 cuando el terminal entra en un modo activo iniciando 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 sencilla en comparación con el manejo de claves modificadas múltiples para estaciones base vecinas de acuerdo con la propuesta de la figura 2. Además, cada clave nueva se crea independientemente en el terminal y en el punto de servicio actual, que transfiere con seguridad la nueva clave al siguiente punto de servicio, suponiendo que se utilicen enlaces de comunicación seguros entre los puntos de servicio. Por lo tanto, ninguna información sensible relacionada con las claves se transmite por aire.

La siguiente figura 3C ilustra una tercera fase en el procedimiento continuo de manejo de claves para cifrado y/o integridad, después de 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 un modo inactivo (por ejemplo, para ahorrar energía de la 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 "camping", aunque sin comunicar datos. Cuando el terminal no está activo, no se necesita ninguna clave naturalmente para la protección y, por lo tanto, no se llevan a cabo 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 iniciando una sesión de comunicación, que está representada por un paso 3:12. Dado que el terminal ya ha sido 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 envía ahora una solicitud de clave para el terminal 300 al nodo 304 de control de servicio, en un siguiente paso 3:13, incluyendo una identidad de terminal. Esta solicitud de clave es normalmente parte de una "solicitud de contexto" más general para el terminal en cuestión, de acuerdo con procedimientos convencionales.

En respuesta a ello, el nodo 304 de control de servicio recupera la clave básica Ik y crea de nuevo una clave modificada inicial Ik'_x en un paso 3:14 aplicando la primera función predeterminada f a al menos la clave básica Ik y el parámetro de versión de clave actualizada v' de 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. De nuevo, una identidad de punto de servicio "SPx" puede opcionalmente también ser introducida en la función f para hacer que la clave Ik'_x sea única para esta combinación de terminal/punto de servicio, así como cualquier otro parámetro.

Debe observarse que incluso si el terminal 300 se reactiva con el mismo punto 302 de servicio como en la figura 3A, resultando en una clave Ik'_1, seguiría siendo diferente de la anterior clave modificada inicial Ik_1 debido al nuevo valor del parámetro de versión de clave v'. En un siguiente paso 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 basado en el valor actualizado v', como se indica en el paso 3:16. Finalmente, la clave Ik'_x puede ahora ser utilizada por el terminal 300 y el punto 308 de servicio para proteger la comunicación durante la sesión, mientras el terminal 300 permanezca conectado al punto 308 de servicio, que se ilustra mediante un 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 totalmente diferente de la cadena anterior. La nueva cadena continuará de la manera descrita anteriormente para la figura 3B al cambiar puntos de servicio, siempre y cuando el terminal permanezca activo, es decir, se aplique en una sesión. Cuando el terminal cambia de un punto de servicio a otro, el antiguo y el terminal pueden borrar su copia de la clave. Por lo tanto, solamente una clave se gestiona a la vez.

Si el terminal permanece activo durante un período relativamente largo, pudiendo resultar potencialmente una disminución de la seguridad, ya que una nueva clave se calcula frecuentemente basándose en la anterior, la seguridad puede restablecerse si se activa una nueva cadena de claves basándose en un parámetro de versión de clave actualizado, incluso si el terminal no ha sido 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 ser activado después de un periodo de tiempo activo preestablecido o después de haber comunicado una cantidad predeterminada de datos, o después de un número predeterminado de cambios de punto 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 una vez que el terminal haya sido cancelado con la red (por ejemplo, cuando esté apagado) y se registre nuevamente o cuando se realice una nueva autenticación. Otra clave básica Ik puede entonces establecerse para el terminal.

Un procedimiento básico de proporcionar claves para un terminal se describirá ahora con referencia al diagrama de flujo ilustrado en la figura 4, 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 se pueden utilizar para proteger la comunicación entre el terminal y los puntos de servicio. Las claves y los parámetros que aparecen en el ejemplo anterior de las figuras 3A-C también se utilizan aquí.

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

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

En un siguiente paso 404, la clave modificada inicial se envía a un primer punto de servicio al que está unido inicialmente el terminal, de manera que puede ser utilizado para proteger la comunicación entre el terminal y el primer punto de servicio.

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

En un siguiente paso 408, una nueva clave modificada inicial Ik'_x se crea por la aplicación de dicha función f a al menos 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, la nueva clave modificada inicial se envía al nuevo punto de servicio, de tal manera que se puede utilizar para proteger la comunicación entre el terminal y el nuevo punto de servicio.

Un procedimiento básico de obtención de claves para un terminal se describirá ahora con referencia al diagrama de flujo ilustrado en la figura 5, como se ejecuta en un primer punto de servicio en una red de comunicación. El terminal se une inicialmente al primer punto de servicio. Las claves y los parámetros que aparecen en el ejemplo anterior de las figuras 3A-C también se utilizan aquí.

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

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

En un siguiente paso 504, una segunda clave modificada Ik_2 se crea por la aplicación de una segunda función predeterminada g a al menos 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 manera que puede ser utilizada para proteger la comunicación entre el terminal y el segundo punto de servicio.

Un procedimiento básico de obtención de claves para proteger la comunicación entre terminal y los puntos de servicio en una red de comunicaciones, se describirá ahora con referencia al diagrama de flujo ilustrado en la figura 6, como se ejecuta en el terminal. El terminal se une inicialmente a un primer punto de servicio en la red. Las claves y los parámetros que aparecen en el ejemplo anterior de las figuras 3A-C también se utilizan aquí.

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

En un siguiente paso 602, una clave modificada inicial Ik_1 se crea por la aplicación de una primera función predeterminada f a al menos 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 manera que puede ser utilizada para proteger la comunicación con el primer punto de servicio.

En un siguiente paso 604, una segunda clave modificada Ik_2 se crea por la aplicación de una segunda función

predeterminada g a al menos la clave modificada inicial Ik_1, si el terminal cambia a un segundo punto de servicio.

En un siguiente paso 606, el terminal se conecta a un nuevo punto de servicio x después de un periodo inactivo con el fin de iniciar una segunda sesión de comunicación.

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

El nodo de control de servicio, punto de servicio y terminal descritos anteriormente en relación con las figuras 4-6 puede estar provisto de medios adecuados para la ejecución de los pasos descritos en los diagramas de flujo mostrados en la figura 4, la figura 5 y la figura 6, respectivamente.

Mediante el uso de la presente solución, por ejemplo de acuerdo con cualquiera de las realizaciones descritas, se obtiene un sencillo mecanismo aún seguro para el manejo de claves para proteger la comunicación entre los terminales y los puntos de servicio en una red de comunicación. Nuevas claves se establecen de forma segura cada vez que el terminal cambia el punto de servicio, y no se requieren predicciones de transferencia. El número de claves que deben ser manejadas por las estaciones base u otros puntos de servicio también se mantiene al mínimo. También se pueden obtener seguridad fiable hacia atrás cuando se cambia los puntos de servicio y seguridad hacia adelante cuando un terminal inicia una sesión, con un mínimo de impacto en el servicio.

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

Aunque la invención se ha descrito con referencia a realizaciones ejemplares específicas, la descripción solamente está destinada a ilustrar el concepto de la invención y no debe tomarse como que limita el alcance de la invención. Diversas alternativas, modificaciones y equivalentes pueden ser utilizadas sin apartarse de la invención, que se define por 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, para proporcionar claves para proteger la comunicación entre un terminal y dichos puntos de servicio, estando caracterizado el método por:

- 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) a un valor inicial de la misma manera que se inicializa por el terminal;

- B) crear (602; 3:2) una clave modificada inicial (Ik_1) aplicando una función predeterminada (f) a al menos la clave básica y el valor inicial del parámetro de versión de clave (v), cuando el terminal inicia una sesión de comunicación, dicha clave modificada inicial (Ik_1) siendo así creada de la misma manera que si fuese creada por el terminal;

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

- D) actualizar (3:14) dicho valor de dicho parámetro de versión de clave (v), cambiándolo de acuerdo con un esquema o algoritmo predeterminado dicho valor actualizado de dicho parámetro de versión de clave (v') siendo de este modo actualizado de la misma manera que si se actualizase por el terminal;

en el que el valor del parámetro de versión de clave (v') se cambia de la misma manera que si se cambiase por el terminal cada vez que se crea una nueva clave modificada inicial.

2.- Un método de acuerdo con la reivindicación 1, que comprende los siguientes pasos adicionales:

- D) recibir (3:13) una solicitud de clave desde un nuevo punto de servicio (x) al que está unido el terminal,

- E) crear (3:14) una nueva clave modificada inicial (Ik'_x) aplicando dicha función a al menos la clave básica y un valor actualizado de dicho parámetro de versión de clave (v'), cuando el terminal inicia una segunda sesión de comunicación, y

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

3.- Un método, como se ejecuta en un terminal inicialmente unido al primer punto de servicio en una red de comunicación, de obtener claves para proteger la comunicación con puntos de servicio en la red, estando caracterizado el método por:

- A) determinar (400; 3:1) una clave básica (Ik) durante un procedimiento de registro al entrar en la red, e inicializar un parámetro de versión de clave (v) a un valor inicial de la misma manera que si se inicializase por el nodo de control de servicio;

- B) crear (402; 3:4) una clave modificada inicial (Ik_1) aplicando una primera función predeterminada (f) a al menos la clave básica y el valor inicial del parámetro de versión de clave (v), al empezar una primera sesión de comunicación, de manera que puede utilizarse para proteger la comunicación con el primer punto de servicio, siendo creada por ello dicha clave modificada inicial (Ik_1) de la misma manera que si se crease por el nodo de control de servicio;

- C) actualizar (408; 3:16) dicho valor de dicho parámetro de versión de clave (v), cambiándolo de acuerdo con un esquema o algoritmo predeterminado dicho valor actualizado de dicho parámetro de versión de clave (v') siendo de este modo actualizado de la misma manera que si se actualizase por el nodo de control de servicio;

en el que el valor del parámetro de versión de clave (v') se cambia de la misma manera que si se cambiase por el nodo de control de servicio cada vez que se crea una nueva clave modificada inicial.

4.- Un método de acuerdo con la reivindicación 3, que comprende los siguientes pasos adicionales:

- D) unir a un nuevo punto de servicio (x) después de un periodo inactivo con el fin de inicial una segunda sesión de comunicación, y

- E) crear una nueva clave modificada inicial (Ik'_x) aplicando dicha primera función a al menos la clave básica y un valor actualizado de dicho parámetro de versión de clave (v'), de manera que se puede utilizar para proteger la comunicación con el nuevo punto de servicio.

5.- Un método de acuerdo con cualquiera de las reivindicaciones 1-4, en el que el parámetro de versión de clave se

inicializa en cero y después se incrementa en uno cada vez que se crea una nueva clave modificada inicial.

6.- Un método de acuerdo con la reivindicación 2, en el que la solicitud de clave se envía cuando el terminal es reactivado después de estar inactivo.

7.- Un método de acuerdo con la reivindicación 2, en el que la solicitud de clave se envía después de que el terminal ha estado activo un periodo de tiempo prestablecido, o ha comunicado una cantidad predeterminada de datos, o ha hecho un número predeterminado de cambios de punto 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, la disposición siendo configurada 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) a un valor inicial de la misma manera que si se inicializase por el terminal;

- crear una clave modificada inicial (Ik_1) aplicando una función predeterminada (f) a al menos la clave básica y el valor inicial del parámetro de versión de clave (v), cuando el terminal inicia una primera sesión de comunicación, dicha clave modificada inicial (Ik_1) siendo creada de este modo como si se crease por el terminal,

- enviar la clave modificada inicial a un primera punto de servicio de dichos puntos de servicio a los que el terminal está unido inicialmente, de manera que puede ser utilizado para proteger la comunicación entre el terminal y el primer punto de servicio, y

- actualizar dicho valor de dicho parámetro de versión de clave (v), cambiándolo de acuerdo con un esquema o algoritmo predeterminado dicho valor actualizado de dicho parámetro de versión de clave (v') siendo actualizado de este modo de la misma manera que si se actualizase por el terminal;

en el que la disposición se configura además para cambiar el valor del parámetro de versión de clave (v') de la misma manera que si se cambiase por el terminal cada vez que se crea una nueva clave modificada inicial.

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

- recibir una solicitud desde un nuevo punto de servicio (x) al que el terminal está unido,

- crear una nueva clave modificada inicial (Ik'_x) aplicando dicha función a al menos la clave básica y un valor actualizado de dicho parámetro de versión de clave (v'), cuando el terminal inicia una segunda sesión de comunicación, y

- enviar la nueva clave modificada inicial al nuevo punto de servicio, de manera que se puede utilizar para proteger la comunicación entre el terminal y el nuevo punto de servicio.

10.- Una disposición en un terminal unido inicialmente a un primer punto de servicio en una red de comunicación, para obtener las claves para proteger la comunicación con los puntos de servicios en la red, la disposición estando configurada 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 del mismo modo que se inicializa por el nodo de control de servicio;

- crear una clave modificada inicial (Ik_1) aplicando una primera función predeterminada (f) a al menos la clave básica y el valor inicial del parámetro de versión de clave (v), cuando se inicia una primera sesión de comunicación, de tal manera que se puede utilizar para proteger la comunicación con el primer punto de servicio, dicha clave modificada inicial (Ik_1) siendo creada de esta manera de la misma forma que si se crease por el nodo de control de servicio;

- actualizar dicho valor de dicho parámetro de versión de clave (v), cambiándolo de acuerdo con un esquema o algoritmo predeterminado dicho valor actualizado de dicho parámetro de versión de clave (v') siendo de este modo actualizado de la misma manera que si se actualizase por el nodo de control de servicio;

configurándose el terminal además para cambiar el valor del parámetro de versión de clave (v') de la misma manera que si se cambiase por el nodo de control de servicio cada vez que se crea una nueva clave modificada inicial.

11.- Una disposición de acuerdo con la reivindicación 10, en el que dicha disposición es además configurada para:

- unirse a un nuevo punto de servicio (x) después de un periodo inactivo con el fin de inicial una segunda sesión de comunicación, y

- crear una nueva clave modificada inicial (Ik'_x) aplicando dicha primera función a al menos la clave básica y un valor actualizado de dicho parámetro de versión de clave (v'), de manera que se puede utilizar para proteger la comunicación con el nuevo punto de servicio.

12.- Una disposición de acuerdo con cualquiera de las reivindicaciones 8-11, en el que dicha disposición se configura además para crear una clave modificada inicial y/o para introducir una identidad de punto de servicio ("SP1", "SPx") en la función predeterminada cuando se crea la clave modificada inicial y/o nueva clave modificada inicial, para hacer la clave única para la combinación particular terminal/punto de servicio.

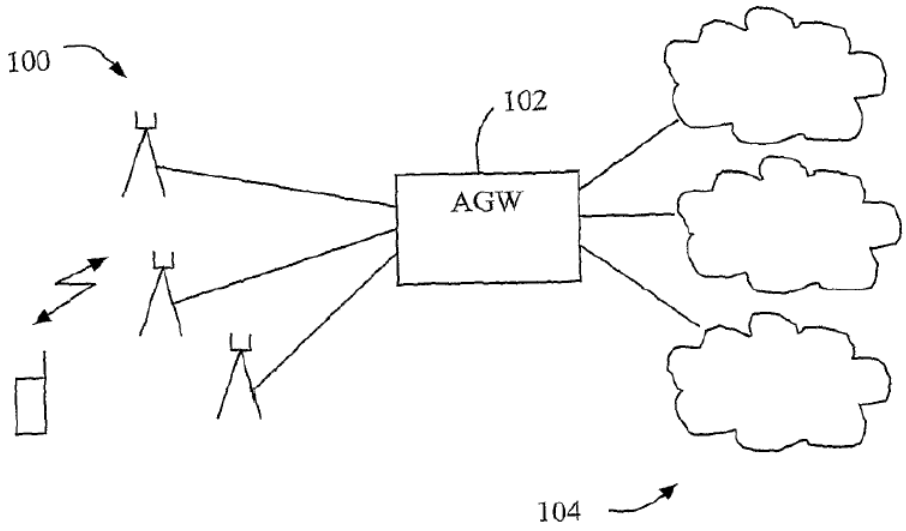
100
102
AGW
104

Fig. 1

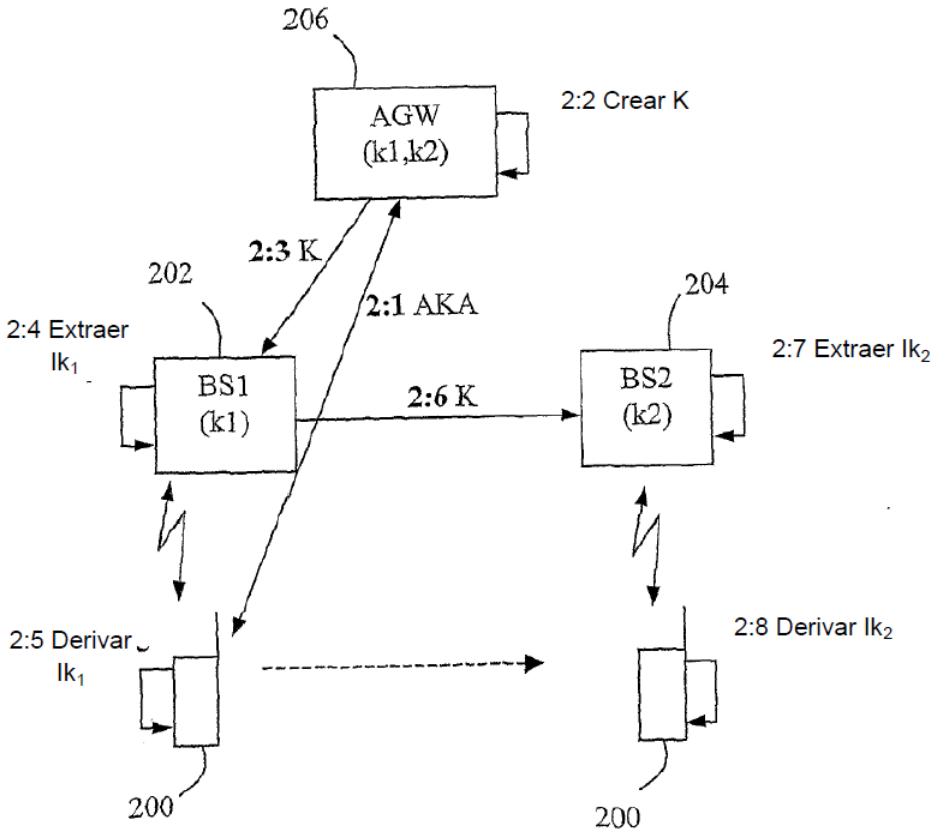
206
AGW
(k1,k2)
2:2 Crear K
2:3 K
202
2:1 AKA
204
2:4 Extraer
Ik1
BS1
(k1)
2:6 K
BS2
(k2)
2:7 Extraer Ik2
2:5 Derivar
Ik1
2:8 Derivar Ik2
200
200

Fig. 2

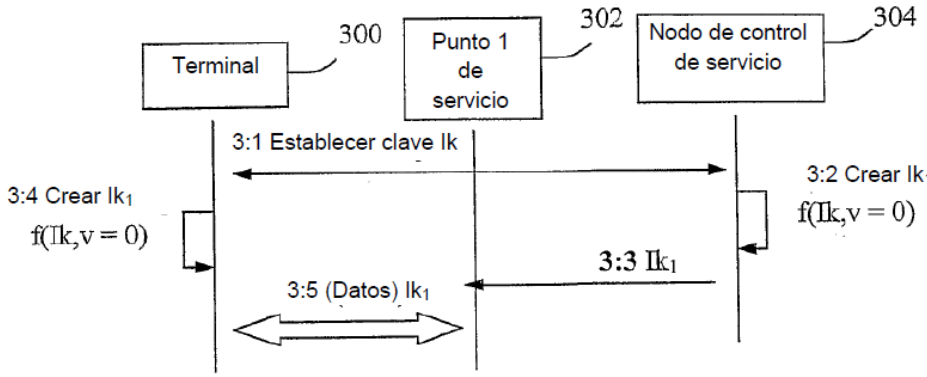

Fig. 3A

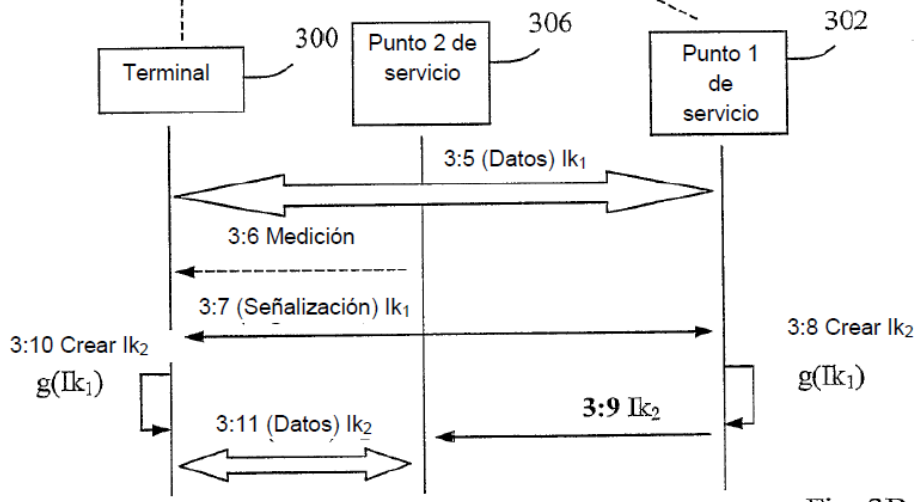

Fig. 3B

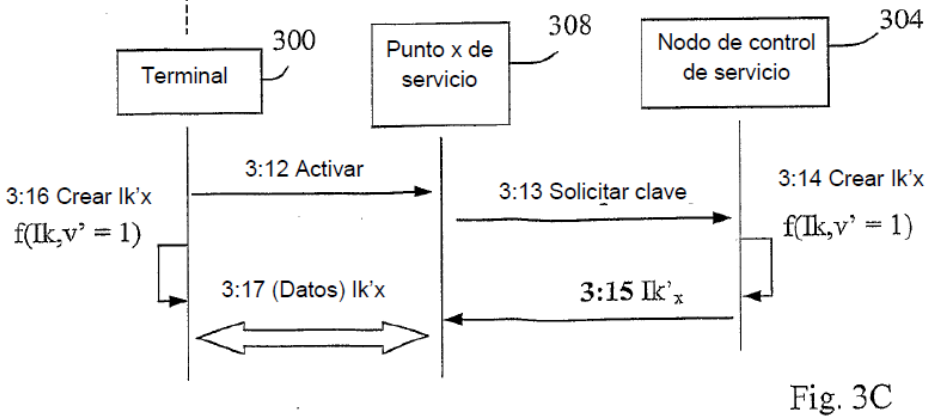

Fig. 3C

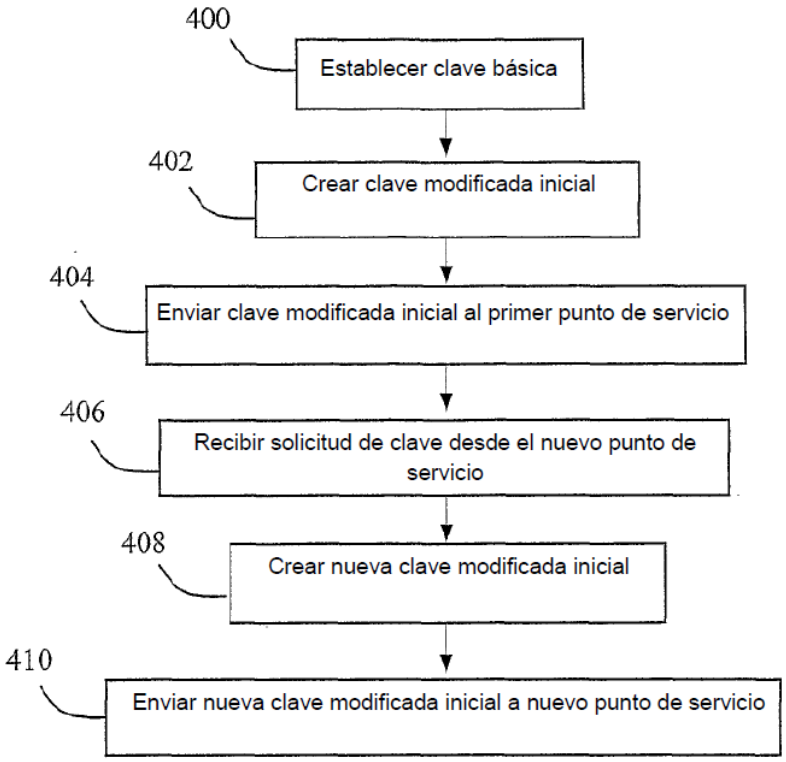
400
Establecer clave básica
402
Crear clave modificada inicial
404
Enviar clave modificada inicial al primer punto de servicio
406
Recibir solicitud de clave desde el nuevo punto de servicio
408
Crear nueva clave modificada inicial
410
Enviar nueva clave modificada inicial a nuevo punto de servicio

Fig. 4

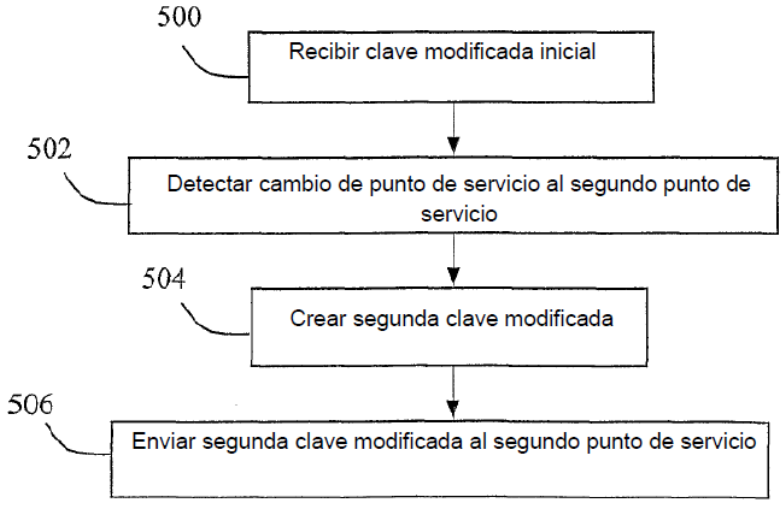
500
Recibir clave modificada inicial
502
Detectar cambio de punto de servicio al segundo punto de servicio
504
Crear segunda clave modificada
506
Enviar segunda clave modificada al segundo punto de servicio

Fig. 5

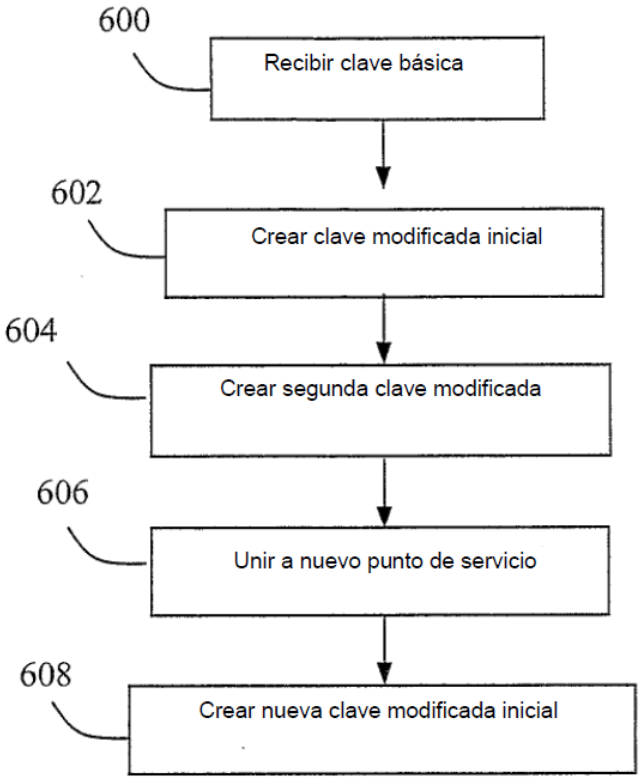
600
Recibir clave básica
602
Crear clave modificada inicial
604
Crear segunda clave modificada
606
Unir a nuevo punto de servicio
608
Crear nueva clave modificada inicial

Fig. 6