(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 662 252**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.04.2003 PCT/IB2003/01655**

(87) Fecha y número de publicación internacional: **20.11.2003 WO03096603**

(96) Fecha de presentación y número de la solicitud europea: **29.04.2003 E 03749966 (2)**

(97) Fecha y número de publicación de la concesión europea: **17.01.2018 EP 1502380**

(54) Título: **Método y sistema de comunicación para el control de la duración de una asociación de seguridad**

(30) Prioridad:

07.05.2002 US 377965 P
16.01.2003 US 345418

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.04.2018

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
KEILALAHDENTIE 4
02150 ESPOO, FI

(72) Inventor/es:

BAJKO, GABOR y
HAUKKA, TAO

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método y sistema de comunicación para el control de la duración de una asociación de seguridad

Antecedentes de la invención

Campo técnico

La presente invención se refiere a la selección de un temporizador de una Asociación de Seguridad (SA) entre un equipo de usuario (UE) y una entidad de control en un sistema de comunicación y en una aplicación preferida de selección de un temporizador de SA para la SA de IPSec entre el UE y una función de control del estado de la llamada de proxy (P-CSCF) en un entorno de comunicaciones 3G.

Técnica anterior

La Fig. 1 ilustra un diagrama de bloques del establecimiento con éxito de unas SA tal como se expone en la sección 7.2 del 3GPP TS 33.203 V5.3.0 (2002-03).

En el dominio de paquetes conmutados, el servicio no se proporciona hasta que se establece una SA entre el UE y el sistema de comunicación 10 tal como la P-CSCF. Un Subsistema de la Red de Núcleo Multimedia IP (IMS) es esencialmente una superposición en el dominio de paquetes conmutados y tiene una baja dependencia del dominio de paquetes conmutados. En consecuencia, se requiere una SA separada entre un UE multimedia (cliente) y el IMS antes de que se conceda el acceso a servicios multimedia.

El procedimiento de establecimiento de la SA es necesario para decidir qué servicios de seguridad aplicar y cuándo han de comenzar los servicios de seguridad en el IMS. En el IMS, la autenticación de los usuarios se realiza durante el registro tal como se especifica en la sección 6.1 de la publicación 3GPP anteriormente citada. Se protege la integridad de las comunicaciones de señalización posteriores en una sesión basándose en claves deducidas durante el proceso de autenticación.

Para protección de la señalización IMS entre el UE y el P-CSCF, es necesario acordar las claves compartidas que se proporcionan por el protocolo de Autenticación y Acuerdo de Claves (AKA) del IMS y un conjunto de parámetros específicos para el método de protección. El modo de seguridad establecido tal como se describe a continuación con referencia a la Fig. 1 se usa para negociar los parámetros de la SA requeridos para autenticación, pero sin confidencialidad. La sección 7.1 de la publicación 3GPP anteriormente citada describe los parámetros de la SA.

La Fig. 1 ilustra el caso normal de establecimiento de las SA usando mensajes del protocolo SIP cuando no tiene lugar un fallo. Algunos de los nodos y mensajes en una arquitectura SIP típica, que no están relacionados directamente con el establecimiento de una SA, se han omitido. En consecuencia, hay huecos en la numeración de mensajes y la Función de Control del Estado de la Llamada de Interrogación (I-CSCF) se ha omitido. El UE envía un mensaje SM1 REGISTER al P-CSCF y hacia la Función de Control del Estado de la Llamada en Servicio (S-CSCF) para registrar la localización del UE y para establecer el modo de seguridad. Para comenzar el procedimiento de establecimiento del modo de seguridad, el UE incluye una línea de establecimiento de seguridad en el mensaje SM1 REGISTER. La línea de establecimiento de seguridad en el SM1 contiene números de la Infraestructura de Aprovisionamiento de Servicio (SPI), el puerto protegido seleccionado por el UE y una lista de identificadores para los algoritmos de integridad que soporta el UE. Tras la recepción del mensaje SM1 REGISTER por el P-CSCF, el P-CSCF almacena temporalmente los parámetros recibidos en la línea de establecimiento de seguridad junto con la dirección IP del UE a partir de la dirección IP de origen de la cabecera del paquete IP, la Identidad Privada IM multimedia (IMPI) IP y la Identidad Pública IM (IMPU). El P-CSCF envía un mensaje SM2 REGISTER al S-CSCF. Tras la recepción por el P-CSCF de un mensaje SM4 4xx Auth_Challenge originado desde el S-CSCF en respuesta al mensaje SM2 REGISTER, el P-CSCF añade la clave IK_{IM} recibida desde el S-CSCF para los parámetros almacenados temporalmente. El P-CSCF selecciona entonces la SPI para la SA entrante. El P-CSCF define las SPI de modo que sean únicas y diferentes respecto a cualquier SPI recibida en la línea de establecimiento de seguridad del UE. Este papel es necesario dado que el UE y el P-CSCF usan la misma clave para el tráfico entrante y saliente. Para determinar la integridad del algoritmo, el P-CSCF procede de modo que el P-CSCF tiene una lista de algoritmos de integridad que soporta el P-CSCF, ordenados por prioridad. El P-CSCF selecciona el primer algoritmo de integridad por sí mismo lo que también está soportado por el UE. El P-CSCF establece entonces otro par de SA en la base de datos de asociaciones de seguridad local. La línea de establecimiento de seguridad en el mensaje SM6 contiene la SPI asignada por el P-CSCF y un número fijo del puerto protegido en el P-CSCF. El mensaje SM6 también contiene una lista de identificadores de los algoritmos de integridad que soporta el P-CSCF. Tras la recepción del mensaje SM6, el UE determina el algoritmo de integridad de modo que el UE selecciona el primer algoritmo de integridad sobre la lista recibida desde el P-CSCF en el mensaje SM6 lo que también está soportado por el UE. El UE procede entonces a establecer otro par de SA. La integridad del UE protege el mensaje SM7 y todos los mensajes SIP siguientes. Se incluye la lista de algoritmos de integridad recibidos en el mensaje SM6. Tras recibir el mensaje SM7 desde el UE, el P-CSCF comprueba si la lista de algoritmos de integridad recibida en el mensaje SM7 es idéntica a la lista de algoritmos de integridad en el mensaje SM6. Si no es este el caso, el

procedimiento de registro se aborta. El P-CSCF incluye en el mensaje SM8 información para el S-CSCF de que el mensaje recibido desde el UE estaba protegido en integridad. El P-CSCF añade esta información a todos los mensajes de registro posteriores recibidos desde el UE que han pasado con éxito la comprobación de integridad en el P-CSCF. El S-CSCF envía un mensaje SM10 2xx Auth_Ok al P-CSCF. El P-CSCF envía un mensaje SM12 2xx Auth_Ok al UE. El mensaje SM12 no contiene información específica para el establecimiento del modo de seguridad (es decir, una línea de establecimiento de seguridad). Sin embargo, cuando el mensaje SM12 no indica ningún error, el P-CSCF confirma que el establecimiento del modo de seguridad ha tenido éxito. Después de la recepción del mensaje SM12 sin indicar ningún error, el UE asume la finalización con éxito del establecimiento del modo de seguridad.

Cada mensaje de registro que incluye un intento de autenticación de usuario produce nuevas SA. Si el intento de autenticación tiene éxito, entonces estas nuevas SA reemplazan a las previas. Si el UE tiene una SA ya activa, entonces el UE usa esta para proteger el mensaje de registro. Si se notifica al S-CSCF por el P-CSCF de que el mensaje de registro desde el UE estaba protegido en integridad, el S-CSCF puede decidir no autenticar el usuario por medio del protocolo AKA. Sin embargo, el UE puede enviar mensajes de registro sin proteger en cualquier momento. En este caso, el S-CSCF autentica al usuario por medio del protocolo AKA. En particular, si el UE tiene una indicación de que la SA ya no está activa en el lado del P-CSCF, el UE envía un mensaje de registro sin proteger. Las SA pueden ser unidireccionales o bidireccionales. Para las SA en la capa IP, la duración se mantiene en la capa de aplicación.

Adicionalmente, el borrado de una SA significa el borrado de la SA tanto desde la capa de aplicación como desde la capa IPsec.

Un UE se implica solamente en un procedimiento de registro a la vez. El UE elimina cualquier dato con relación a cualesquiera registros o autenticaciones incompletos previos, incluyendo las SA creadas por una autenticación incompleta. El UE puede comenzar un procedimiento de registro con un par de SA existentes. Se hace referencia a estas SA como unas SA antiguas. La autenticación produce un par de SA nuevas. Estas nuevas SA no se deberán usar para proteger el tráfico no de autenticación hasta que se detecten durante la autenticación del flujo. De la misma manera, ciertos mensajes en la autenticación están protegidos con una SA particular. Si el UE recibe el mensaje protegido con una SA incorrecta, descartará el mensaje.

El RFC 3261, que esencialmente corresponde a draft-ietf-sip-rfc2543bis-09, describe el protocolo SIP. Como se describe en la sección 10.3 del mismo, cuando un UE envía un mensaje REGISTER, un solicitante del registro, que puede ser el P-CSCF, procesa la solicitud. El mensaje REGISTER tiene una dirección de Contacto y un campo de cabecera de Contacto para cada dirección.

La determinación del tiempo de expiración del registro de un UE es como sigue:

(1) Si el campo valor tiene un parámetro de expiración, debe usarse ese valor.
(2) Si no hay tal parámetro, pero la solicitud tiene un campo de cabecera de Expiración, debe usarse ese valor.
(3) Si no hay ninguno de los dos, debe usarse un valor por omisión configurado localmente. El registrado puede acortar el intervalo de expiración.

Con el protocolo SIP, el denominado “temporizador de tiempo de transacción no-INVITE” es de 32 segundos. Este temporizador se usa como un temporizador provisional cuando se envían los mensajes SM4 y SM6 tal como se ha descrito anteriormente. El UE tiene 30 segundos para enviar el mensaje SM7 REGISTER, que contiene la respuesta al mensaje SM6 4xx Auth_Challenge por parte de la red. Cuando el desafío de autenticación en el mensaje SM6 es respondido a tiempo con los mensajes SM7 y SM8 REGISTER y el resultado se verifica por la red, se envía una respuesta SIP 200 Ok al UE con los mensajes SM10 y SM12 descritos anteriormente. El mensaje 200 Ok contiene una cabecera de Expiración o un campo de Contacto descritos anteriormente que indican la duración temporal del registro del UE con la entidad de control.

En la técnica anterior, el temporizador de SA puede fijarse bastante largo, lo que da como resultado ineficiencia en la red en la gestión de bases de datos y la oportunidad de que el UE ataque por desbordamiento el P-CSCF con mensajes que requieren una respuesta apropiada. Si el UE no tiene una SA con la red, dichos mensajes no alcanzan al P-CSCF que es preferido por los operadores de la red debido a un uso más eficiente de recursos.

En sistemas de comunicación 3G, el UE ha de registrarse y re-registrarse de vez en cuando. Cuando el re-registro no es solicitado dentro de un tiempo especificado, los datos del abonado se borran de los elementos de red responsables del manejo de las comunicaciones a y desde el UE, tales como el P-CSCF. Por lo tanto, se mantiene un temporizador de registro en el UE para determinar cuándo es apropiado un re-registro.

Sumario de la invención

De acuerdo con diversos aspectos de la presente invención, se proporciona un método que tiene las características de la reivindicación 1, un aparato que tienen las características de la reivindicación 6, un método que tienen las

características de la reivindicación 11 y un aparato que tienen las características de la reivindicación 12. Se definen realizaciones ventajosas de las mismas en las reivindicaciones dependientes respectivas.

La presente invención *comprende* un método para la selección de una duración de tiempo de una(s) SA entre un UE que transmite y recibe comunicaciones y una entidad de control en un sistema de comunicación y un sistema de comunicación en el que la duración de una(s) SA se fija con suficiente tiempo para permitir la finalización del registro. Este objetivo se lleva a cabo con la invención mediante el ajuste de la duración de cada nueva(s) SA igual al tiempo de duración del temporizador de registro lo que determina el límite de tiempo en el que un registro de un UE es inválido. La(s) SA *puede(n)* fijarse para comunicaciones bidireccionales entre el UE y la entidad de control del sistema de comunicación. En una realización preferida, la entidad de control es el P-CSCF. También, de acuerdo con *una realización preferida* de la invención, una antigua SA continúa durante un intervalo más que cuando debería tener lugar el borrado cuando se fija una nueva SA con una duración de tiempo igual a los tiempos de registro.

De acuerdo con una realización preferida de la invención que usa el protocolo SIP, se envía el mensaje SM1 REGISTER por el UE para registrar el UE con el IMS en el P-CSCF. Si el mensaje SM1 está protegido, está protegido con una SA saliente antigua. El UE recibe un desafío de autenticación en un mensaje SM6 desde el P-CSCF que está protegido con la SA saliente antigua si el mensaje SM1 está protegido y estaría desprotegido en caso contrario. Si el mensaje SM6 puede procesarse con éxito por el UE, el UE crea al menos una nueva SA, que se deduce de acuerdo con los parámetros de asociación de seguridad de la sección 7.1 del 3GPP TS 33.203 V. 5.3.0 (2002-09). La duración de cada nueva SA creada en este momento se fija para permitir un tiempo suficiente para completar el procedimiento de registro. El UE envía un mensaje SM7 antes de la expiración de un valor de temporizador provisional enviado en los mensajes SM4 y SM6 al P-CSCF que están protegidos con la nueva SA saliente. El P-CSCF envía un mensaje SM8 al S-CSCF. Si el mensaje SM1 está protegido, las nuevas SA pueden usarse ahora para proteger mensajes distintos de los de la autenticación. Adicionalmente, para el tráfico saliente, se usa la nueva SA. El S-CSCF envía un mensaje SM10 al P-CSCF que usa el valor del temporizador de registro contenido en la cabecera de Expiración o Contacto para fijar el tiempo de duración de la nueva SA en el P-CSCF. El UE recibe el mensaje SM12 desde el P-CSCF indicando la autenticación con éxito desde el P-CSCF que está protegida con la nueva SA saliente. El UE usa el valor del tiempo de registro contenido en la cabecera de Expiración o Contacto para fijar la duración de tiempo de la nueva SA en el. Después del procesamiento con éxito del mensaje por el UE, el registro está completo. Las antiguas SA se borran ahora u opcionalmente pueden retenerse durante un intervalo más y las nuevas SA se usan para proteger todos los mensajes y tienen una duración de tiempo igual a la longitud de tiempo del valor del temporizador de registro contenido de los mensajes SM10 y SM12.

La presente invención elimina los problemas de la técnica anterior mediante la eliminación del desbordamiento del P-CSCF con mensajes cuando la duración del tiempo de las nuevas SA no se fijó para que tuviera ninguna duración de tiempo particular con respecto al temporizador de registro y tenía una duración de tiempo más larga que el temporizador de registro para que el UE se registre con la entidad de control del sistema de comunicación. Como resultado de la invención, se mejora la eficiencia del sistema de comunicación de acuerdo con la presente invención.

Un método para seleccionar una longitud de tiempo de una asociación de seguridad entre un equipo de usuario que transmite y recibe comunicaciones y una entidad de control en un sistema de comunicación de acuerdo con la invención incluye transmitir un mensaje de registro desde el equipo de usuario a la entidad de control solicitando el registro del equipo de usuario con la entidad de control; después de la transmisión del mensaje de registro, fijar la longitud de tiempo de la asociación de seguridad entre el equipo de usuario y la entidad de control para que sea igual a una longitud del temporizador de registro fijada entre el equipo de usuario y la entidad de control durante la que es válido el registro del equipo de usuario con la entidad de control; y transmitir la longitud de tiempo fijada de la asociación de seguridad al equipo de usuario como parte de un mensaje de acuse de recibo al mensaje de registro para hacer que la asociación de seguridad tenga un tiempo igual al temporizador de registro. La entidad de control puede realizar una función de control del estado de llamada en el sistema de comunicación. Las comunicaciones entre el equipo de usuario y el sistema de comunicación pueden usar el Protocolo de Inicio de Sesión (SIP) y el mensaje de registro puede ser un mensaje de solicitud SIP REGISTER y el mensaje de acuse de recibo puede ser un mensaje de respuesta SIP 2xx. Puede enviarse un desafío de autenticación que incluye un temporizador provisional al equipo de usuario, precediendo al acuse de recibo, lo que fija un tiempo de duración para que el equipo de usuario responda al desafío de autenticación. Puede enviarse un mensaje de registro desde el equipo de usuario a la entidad de control en un mensaje de respuesta al desafío de autenticación dentro de la duración de tiempo fijada por el equipo de usuario para responder al desafío de autenticación. La duración de tiempo puede estar contenida en una cabecera de Expiración o de Contacto del protocolo SIP. El temporizador provisional puede ser un temporizador de tiempo de transacción no INVITE del protocolo SIP.

Un sistema de comunicación de acuerdo con la invención que incluye un equipo de usuario que transmite y recibe comunicaciones y una entidad de control que proporciona funciones de control en el sistema de comunicación, y en el que se transmite un mensaje de registro desde el equipo de usuario a la entidad de control solicitando el registro del usuario con la entidad de control; después de la transmisión del mensaje de registro, la longitud de tiempo de la asociación de seguridad entre el equipo de usuario y la entidad de control se fija para que sea igual a una longitud de tiempo de un temporizador de registro fijada entre el equipo de usuario y la entidad de control durante la que es válido el registro del equipo de usuario con la entidad de control; y la longitud de tiempo fijada de la asociación de

seguridad se transmite desde la entidad de control al equipo de usuario como un mensaje de acuse de recibo al mensaje de registro para hacer que la asociación de seguridad tenga una duración de tiempo igual al temporizador de registro. La entidad de control puede realizar una función de control del estado de llamada en el sistema de comunicación. Las comunicaciones entre el equipo de usuario y el sistema de comunicación pueden usar el Protocolo de Inicio de Sesión (SIP) y el mensaje de registro puede ser un mensaje de solicitud SIP REGISTER y el mensaje de acuse de recibo puede ser un mensaje de respuesta SIP 2xx. Puede enviarse un desafío de autenticación que incluye un temporizador provisional al equipo de usuario, precediendo al acuse de recibo, lo que fija una duración de tiempo para que el equipo de usuario responda al desafío de autenticación. Puede enviarse un mensaje de registro desde el equipo de usuario a la entidad de control en un mensaje de respuesta al desafío de autenticación dentro de la duración de tiempo fijada por el equipo de usuario para responder al desafío de autenticación. La duración de tiempo puede estar contenida en uno de una cabecera de Expiración o de Contacto del protocolo SIP. El temporizador provisional puede ser un temporizador de tiempo de transacción no INVITE del protocolo SIP.

Breve descripción de los dibujos

La Fig. 1 ilustra el registro de la técnica anterior de un UE en un sistema de comunicación que usa el protocolo SIP que incluye en él las entidades de control P-CSCF y S-CSCF.

La Fig. 2 ilustra un método de fijación de la duración de tiempo de una(s) nueva(s) SA para que sea igual al temporizador de registro que controla el registro de un UE como en el sistema de la técnica anterior de la Fig. 1.

Partes iguales se identifican de modo idéntico en las Figs. 1 y 2.

Mejor modo para llevar a cabo la invención

Se describe en conjunto con la Fig. 2 un sistema de comunicación y un método que fija las SA para que tengan una duración del temporizador igual a la del temporizador de registro que define cuándo el registro de un UE es válido de acuerdo con la invención. Aunque la invención se ha descrito con referencia al protocolo SIP, debería entenderse que la invención no está limitada al mismo.

La primera etapa en la Fig. 2 es que el UE envíe un mensaje de registro a una entidad de control del sistema de comunicación solicitando el registro del UE. La entidad de control en una realización preferida es un P-CSCF y el mensaje de registro es el mensaje SM1 SIP REGISTER transmitido al P-CSCF de acuerdo con la técnica anterior. El P-CSCF envía el mensaje de registro que preferentemente es el mensaje SM2 SIP REGISTER, al S-CSCF. El S-CSCF envía un mensaje de desafío de autenticación que preferentemente es el mensaje SIP SM4 mensaje 4xx AUTH-Challenge al P-CSCF. El P-CSCF envía un mensaje de desafío de autenticación, que es preferentemente el SM6 4xx AUTH-Challenge del protocolo SIP, al UE. Los mensajes de desafío de autenticación SM4 y SM6 incluyen un temporizador provisional que fija un límite de tiempo para que el UE transmita el mensaje de registro, que preferentemente es el mensaje SM7 REGISTER del protocolo SIP, en respuesta al mensaje SM6 de desafío de autenticación. En una realización de la invención, el valor del temporizador provisional se fija igual a 32 segundos, que es el temporizador de tiempo de transacción no INVITE del protocolo SIP. El P-CSCF determina mediante el procesamiento del mensaje SM7 si el UE ha respondido dentro del valor del temporizador provisional. Si el temporizador provisional expira, el proceso de registro y la fijación de la SA se abortan. El P-CSCF envía entonces un mensaje de registro, que es preferentemente el mensaje SM8 REGISTER del protocolo SIP, al S-CSCF. El S-CSCF fija la longitud de tiempo de su SA para el P-CSCF igual al límite del temporizador de registro contenido en el mensaje SM8. El límite de tiempo fijado para la SA, que es igual al temporizador de registro, se envía como parte del mensaje SM10 al P-CSCF y a continuación, desde el P-CSCF como el mensaje SM12, al UE. Cuando la invención se pone en práctica con el protocolo SIP, los Campos Expiración o Contacto pueden usarse para contener el límite de temporizador fijado para las nuevas SA. El P-CSCF también fija su intervalo de tiempo de SA para que sea igual al intervalo del temporizador de registro. El P-CSCF envía el valor fijado de su temporizador de SA, que es igual al temporizador de registro, al UE. El UE fija un límite de tiempo para su SA para comunicaciones con el P-CSCF para que sea igual a una longitud del temporizador de registro fijada por el UE que define cuándo es válido el registro del UE con la entidad de control. La longitud de tiempo de las SA es para comunicaciones bidireccionales entre el P-CSCF y el UE. La invención no está limitada al límite de tiempo de SA que se envía mediante los mensajes SM10 y SM12 y no está limitada al uso de las cabeceras de Expiración y Contacto para transmitir el límite de tiempo de SA al P-CSCF y al UE. El límite de tiempo se transmite preferentemente como parte del mensaje de acuse de recibo que, en una realización preferida, son los mensajes SM10 y SM12 del protocolo SIP, que son sensibles al mensaje de registro SM8 recibido por el S-CSCF. La fijación de una o más SA iguales a la longitud de tiempo del temporizador de registro entre el UE y el P-CSCF asegura que se elimina el problema de la técnica anterior de desbordamiento del P-CSCF con mensajes, tal como se ha descrito anteriormente.

Aunque la presente invención se ha descrito en términos de sus realizaciones preferidas, debería entenderse que pueden realizarse a la misma numerosas modificaciones sin apartarse del alcance de la presente invención tal como se define por las reivindicaciones adjuntas. Se pretende que todas las dichas modificaciones caen dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método, que comprende:

recibir un mensaje de registro desde un equipo de usuario, en el que el mensaje de registro es para la solicitud de registro del equipo de usuario con una entidad de control en un sistema de comunicación;
después de recibir el mensaje de registro, fijar una longitud de tiempo de una asociación de seguridad entre el equipo de usuario y la entidad de control para que sea igual a una longitud de tiempo de registro fijada para el registro del equipo de usuario con la entidad de control;
en respuesta al mensaje de registro transmitir al equipo de usuario un desafío de autenticación que comprende un temporizador provisional, precediendo a un mensaje de acuse de recibo, que fija una duración de tiempo para que el equipo de usuario responda al desafío de autenticación,
recibir un mensaje de respuesta desde el equipo de usuario y determinar si el equipo de usuario ha respondido dentro de la duración de tiempo fijada para que el equipo de usuario responda al desafío de autenticación, y
si el equipo de usuario ha respondido dentro de la duración de tiempo fijada, transmitir al equipo de usuario la longitud de tiempo fijada de la asociación de seguridad como parte del mensaje de acuse de recibo al mensaje de registro para hacer que la asociación de seguridad tenga una longitud de tiempo igual a la longitud del tiempo de registro;
en el que las comunicaciones entre el equipo de usuario y el sistema de comunicación se configuran para usar un protocolo de inicio de sesión, y
en el que el mensaje de registro comprende un mensaje de solicitud de registro del protocolo de inicio de sesión y el mensaje de acuse de recibo comprende un mensaje de respuesta del protocolo de inicio de sesión.

2. Un método de acuerdo con la reivindicación 1, que comprende adicionalmente:

realizar una función de control del estado de llamada en el sistema de comunicación.

3. Un método de acuerdo con las reivindicaciones 1 o 2 en el que:

el mensaje de respuesta del protocolo de inicio de sesión es un mensaje 200 Auth_Ok.

4. Un método de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en el que:

la duración de tiempo está contenida en uno de entre una cabecera de expiración o de contacto del protocolo de inicio de sesión.

5. Un método de acuerdo con una cualquiera de las reivindicaciones 1 a 4, en el que:

el temporizador provisional es un temporizador de tiempo de transacción no-invite del protocolo de inicio de sesión.

6. Un aparato, que comprende:

medios de recepción para recibir un mensaje de registro desde un equipo de usuario, en donde el mensaje de registro es para la solicitud de registro del equipo de usuario con el aparato;
medios de fijación para fijar, después de la recepción del mensaje de registro, una longitud de tiempo de una asociación de seguridad entre el equipo de usuario y el aparato para que sea igual a una longitud de tiempo de una longitud de tiempo de registro fijada para un registro del equipo de usuario con el aparato; y
medios de transmisión para transmitir al equipo de usuario la longitud de tiempo fijada de la asociación de seguridad como parte de un mensaje de acuse de recibo al mensaje de registro para hacer que la asociación de seguridad tenga una longitud de tiempo igual a la longitud del tiempo de registro, y para transmitir al equipo de usuario un desafío de autenticación que comprende un temporizador provisional, precediendo al mensaje de acuse de recibo, que fija una duración de tiempo para que el equipo de usuario responda al desafío de autenticación,
en el que las comunicaciones entre el equipo de usuario y el aparato están configuradas para usar un protocolo de inicio de sesión,
en el que el mensaje de registro comprende un mensaje de solicitud de registro del protocolo de inicio de sesión y el mensaje de acuse de recibo comprende un mensaje de respuesta del protocolo de inicio de sesión,
en el que los medios de recepción son además para recibir un mensaje de respuesta desde el equipo de usuario dentro de la duración de tiempo fijada para que el equipo de usuario responda al desafío de autenticación,
en el que el aparato está configurado para determinar si el equipo de usuario ha respondido dentro de la duración de tiempo fijada para que el equipo de usuario responda al desafío de autenticación y para transmitir el mensaje de acuse de recibo si el equipo de usuario ha respondido dentro de la duración de tiempo fijada.

7. Un aparato de acuerdo con la reivindicación 6, en el que:

el aparato está configurado para realizar una función de control del estado de llamada en un sistema de comunicación.

8. Un aparato de acuerdo con la reivindicación 6 o la reivindicación 7, en el que:

el mensaje de respuesta del protocolo de inicio de sesión es un mensaje 200 Auth_Ok.

9. Un aparato de acuerdo con una cualquiera de las reivindicaciones 6 a 8, en el que:

la duración de tiempo está contenida en uno de entre una cabecera de expiración o de contacto del protocolo de inicio de sesión.

10. Un aparato de acuerdo con una cualquiera de las reivindicaciones 6 a 9, en el que:

el temporizador provisional es un temporizador de tiempo de transacción no-invite del protocolo de inicio de sesión.

11. Un método, que comprende:

transmitir un mensaje de registro a una entidad de control en un sistema de comunicación, en donde el mensaje de registro es para la solicitud de registro de un equipo de usuario con la entidad de control;
recibir desde la entidad de control, en respuesta al mensaje de registro, un desafío de autenticación que comprende un temporizador provisional, precediendo a un mensaje de acuse de recibo, que fija una duración de tiempo para que el equipo de usuario responda al desafío de autenticación,
transmitir un mensaje de respuesta dentro de la duración de tiempo;
recibir, desde la entidad de control, una longitud de tiempo fijada de una asociación de seguridad entre el equipo de usuario y la entidad de control como parte del mensaje de acuse de recibo al mensaje de registro para hacer que la asociación de seguridad tenga una longitud de tiempo igual a una longitud de tiempo de registro fijada para un registro del equipo de usuario con la entidad de control; y
después de recibir el mensaje de acuse de recibo, fijar la longitud de tiempo fijada de la asociación de seguridad para que sea igual a la longitud de tiempo de registro fijada para un registro del equipo de usuario con la entidad de control;
en el que las comunicaciones entre el equipo de usuario y el sistema de comunicación se configuran para usar un protocolo de inicio de sesión, y
en el que el mensaje de registro comprende un mensaje de solicitud de registro del protocolo de inicio de sesión y el mensaje de acuse de recibo comprende un mensaje de respuesta del protocolo de inicio de sesión.

12. Un aparato, que comprende:

medios de transmisión para transmitir un mensaje de registro a una entidad de control en un sistema de comunicación, en donde el mensaje de registro es para la solicitud de registro del aparato con la entidad de control; en donde los medios de transmisión son además para transmitir dentro de una duración de tiempo un mensaje de respuesta a la entidad de control en respuesta a un desafío de autenticación desde la entidad de control;
medios de recepción para recibir, desde la entidad de control, una longitud de tiempo fijada de una asociación de seguridad entre el aparato y la entidad de control como parte de un mensaje de acuse de recibo al mensaje de registro para hacer que la asociación de seguridad tenga una longitud de tiempo igual a una longitud de tiempo de registro fijada para un registro del equipo de usuario con la entidad de control, y para recibir desde la entidad de control, en respuesta al mensaje de registro, el desafío de autenticación que comprende un temporizador provisional, precediendo al mensaje de acuse de recibo, que fija la duración de tiempo para que el equipo de usuario responda al desafío de autenticación; y
después de recibir el mensaje de acuse de recibo, fijar la longitud de tiempo fijada de la asociación de seguridad para que sea igual a la longitud de tiempo de registro fijada para el registro del aparato con la entidad de control;
en donde las comunicaciones entre el aparato y el sistema de comunicación están configuradas para usar un protocolo de inicio de sesión, y
en donde el mensaje de registro comprende un mensaje de solicitud de registro del protocolo de inicio de sesión y el mensaje de acuse de recibo comprende un mensaje de respuesta del protocolo de inicio de sesión.

FIG. 1
(TÉCNICA ANTERIOR)

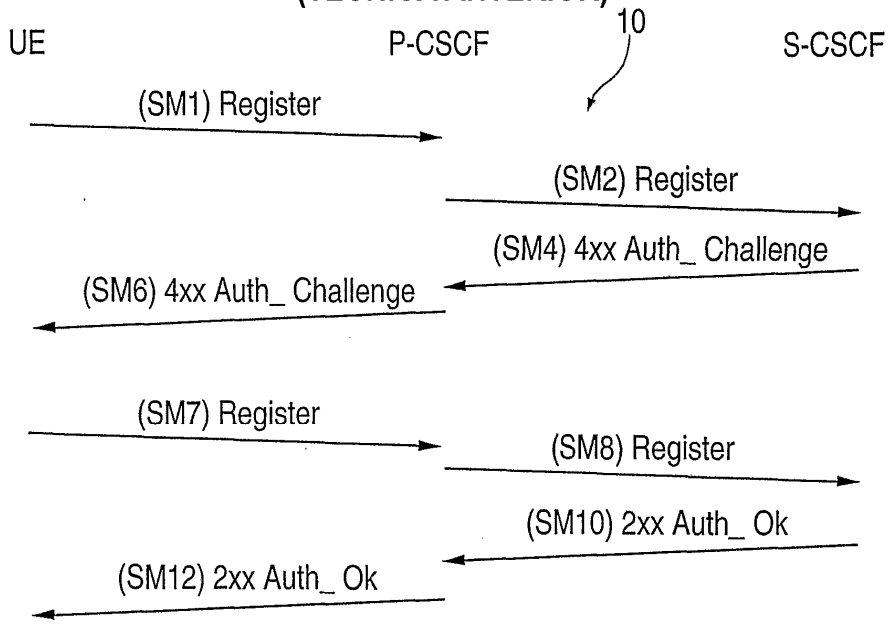

FIG. 2