(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 515 815**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.12.2003 E 03779653 (9)**

(97) Fecha y número de publicación de la concesión europea: **30.07.2014 EP 1653661**

(54) Título: **Método de autenticación para pasarela médica**

(30) Prioridad:

05.08.2003 CN 03149767

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.10.2014

(73) Titular/es:

ZTE CORPORATION (100.0%)
ZTE PLAZA, KEJI ROAD SOUTH, HI-TECH INDUSTRIAL PARK, NANSHAN DISTRICT
518057 SHENZHEN, GUANGDONG, CN

(72) Inventor/es:

QIAO, KEZHI y
NI, MING

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Método de autenticación para pasarela médica

Campo técnico de la invención

La presente invención se refiere a la técnica de comunicación, y más particularmente, a un método de autenticación para Pasarela de Medios con el protocolo de MEGACO/MGCP.

Antecedentes de la invención

El protocolo de Control de Pasarela de Medios (MEGACO) es el protocolo del RFC3015 del Grupo Especial sobre Ingeniería de Internet (IETF).

La Figura 1 muestra un diagrama de interconexiones de red del sistema para conseguir el protocolo de MEGACO. El protocolo de MEGACO emplea una idea de separar la pasarela, que divide una señalización de procesamiento de pasarela y medios juntos en dos partes: la Pasarela de Medios (MG) y el Controlador de Pasarela de Medios (MGC). El MGC controla la operación de la MG mediante el protocolo de MEGACO de tal manera que el MGC envía un comando para llevarse a cabo a la MG, y a continuación la MG lo lleva a cabo y devuelve el resultado. El MGC procesa también peticiones de eventos enviadas de manera iniciativa mediante la MG. La relación lógica en el protocolo de MEGACO se expresa mediante un modelo de conexión. Dos componentes básicos del modelo de conexión son contextos y terminaciones. El contexto expresa la relación de conexión y topografía entre las terminaciones.

Los comandos principales entre el MGC y la MG incluyen CAMBIO DE SERVICIO (SERVICECHANGE), AÑADIR (ADD), MODIFICAR (MODIFY), RESTAR (SUBTRACT), NOTIFICAR (NOTIFY) y así sucesivamente.

En un método convencional de autenticación para la Pasarela de Medios, después de que ha finalizado el registro de la MG, la MG se autentica periódicamente usando una clave constante. Esto tiene varias desventajas de manera que en primer lugar si se usa la misma clave para autenticación durante un largo tiempo, es fácil de decodificar por terceros. En segundo lugar, en el método de autenticación periódica, es fácil para terceros hacer autenticación satisfactoria entre el MGC y la MG únicamente filtrando el mensaje de autenticación a la MG real, e iniciar una llamada falsificando otros mensajes de la MG. En tercer lugar, en el método, únicamente el MGC autentica a la MG, por lo tanto puede llamarse a la MG mediante el MGC inválido falsificando mensajes.

Adicionalmente, la técnica anterior es la norma del ETSI DTS-AT-020020-11 Versión 0.1.3.

Sumario de la invención

Un objeto de la presente invención es proporcionar un método de autenticación mejorado para la Pasarela de Medios, que resuelve los problemas en el método de autenticación convencional para la Pasarela de Medios de manera que es fácil para terceros iniciar una llamada falsificando la MG, llamar a la MG falsificando el MGC, y decodificar la clave puesto que el tiempo de vida de la misma es corto. El método puede autenticar cada llamada, actualizar una clave compartida periódicamente y evitar llamar usando mensajes falsificados inválidos eficazmente.

La presente invención se consigue mediante:

La presente invención desvela un método de autenticación para la Pasarela de Medios, que comprende: establecer una clave inicial para validar firmas digitales iniciales entre una Pasarela de Medios y un Controlador de Pasarela de Medios; generar una nueva clave compartida que tiene un tiempo de vida específico realizando comunicación de señalización entre dicha Pasarela de Medios y dicho Controlador de Pasarela de Medios con dicha clave inicial; autenticar llamadas y respuestas entre dicha Pasarela de Medios y dicho Controlador de Pasarela de Medios con dicha nueva clave compartida; y actualizar dicha clave compartida entre dicha Pasarela de Medios y dicho Controlador de Pasarela de Medios si el tiempo de vida de dicha clave ha expirado.

Preferentemente, la etapa de generación de una nueva clave compartida comprende adicionalmente: iniciar una señalización de registro desde dicha Pasarela de Medios a dicho Controlador de Pasarela de Medios para registro, en el que dicha señalización de registro tiene un parámetro para generar una clave compartida y una firma digital generada mediante dicha clave inicial; generar una clave compartida y establecer un tiempo de vida de dicha clave compartida después de que dicho Controlador de Pasarela de Medios ha validado dicha Pasarela de Medios con dicha clave inicial; iniciar un comando de modificación desde dicho Controlador de Pasarela de Medios a dicha Pasarela de Medios, en el que dicho comando de modificación tiene un parámetro para generar la clave compartida, una firma digital generada mediante dicha clave inicial y un tiempo de vida de una clave compartida; y generar la clave compartida y establecer el tiempo de vida de dicha clave compartida después de que dicha Pasarela de Medios ha validado dicho Controlador de Pasarela de Medios con dicha clave inicial.

Preferentemente, la etapa de autenticación comprende adicionalmente: para cada llamada, adjuntar una firma digital a cada mensaje de llamada desde dicho Controlador de Pasarela de Medios a dicha Pasarela de Medios usando dicha clave compartida; validar dicha firma digital en dicho mensaje de llamada en dicha Pasarela de Medios usando dicha clave compartida, y si es válida, devolver un mensaje de respuesta adjunto con una firma digital usando dicha clave compartida a dicho Controlador de Pasarela de Medios; y validar dicha firma digital en dicho mensaje de respuesta en dicho Controlador de Pasarela de Medios usando dicha clave compartida, si es válida, establecer un servicio de llamada, de otra manera denegar la llamada.

Preferentemente, la etapa de actualización de dicha clave compartida comprende adicionalmente: enviar un comando de notificación desde dicha Pasarela de Medios a dicho Controlador de Pasarela de Medios, pedir a dicho Controlador de Pasarela de Medios generar una nueva clave compartida, en el que dicho comando de notificación tiene un parámetro para generar una clave compartida y una firma digital generada mediante una clave inicial; generar una nueva clave compartida y establecer un tiempo de vida de dicha clave compartida después de que dicho Controlador de Pasarela de Medios ha validado dicha Pasarela de Medios con dicha clave inicial; iniciar un comando de modificación desde dicho Controlador de Pasarela de Medios a dicha Pasarela de Medios, en el que dicho comando de modificación tiene un parámetro para generar la clave compartida, una firma digital generada mediante dicha clave inicial y el tiempo de vida de la clave compartida; y generar la clave compartida y establecer el tiempo de vida de dicha clave compartida después de que dicha Pasarela de Medios ha validado dicho Controlador de Pasarela de Medios con dicha clave inicial.

Preferentemente, el algoritmo usado para generar una clave compartida mediante dicho Controlador de Pasarela de Medios y dicha Pasarela de Medios es diferente del algoritmo usado para generar una firma digital mediante dicho Controlador de Pasarela de Medios y dicha Pasarela de Medios.

Preferentemente, se usa un campo/paquete de un protocolo expandido para transmitir dicho parámetro para generar una clave compartida y dicha firma digital.

Preferentemente, el tiempo de vida de dicha clave compartida es el tiempo, o el número de veces que puede usarse dicha clave compartida para autenticación.

Los efectos ventajosos del presente método son que: el método no puede actualizar únicamente una clave compartida periódicamente de modo que no es fácil de decodificar una clave puesto que la clave se usa durante un tiempo largo, autentica cada llamada iniciada mediante la MG y resuelve el problema de que se inicia una llamada inválida mediante terceros filtrando mensajes, pero evita también que se llame a la MG mediante MGC inválidos.

Breve descripción de los dibujos

La Figura 1 muestra un diagrama de los principios del sistema del protocolo de MEGACO.
La Figura 2 es un diagrama de flujo que muestra un método de autenticación para la Pasarela de Medios de la presente invención.

Descripción detallada de las realizaciones preferidas

La presente invención desvela un método de autenticación para la Pasarela de Medios, que comprende:

establecer el algoritmo usado para generar una clave compartida mediante un Controlador de Pasarela de Medios y una Pasarela de Medios si $y=f_1(x)$, y establecer el algoritmo usado para generar una firma digital mediante un Controlador de Pasarela de Medios y una Pasarela de Medios si $y=f_2(x)$; el algoritmo apropiado puede usarse para el algoritmo usado para generar una clave compartida mediante un Controlador de Pasarela de Medios y una Pasarela de Medios y el algoritmo usado para generar una firma digital mediante un Controlador de Pasarela de Medios y una Pasarela de Medios de acuerdo con el nivel de seguridad requerido, y no puede definirse mediante la presente invención.

Una clave S para validar firmas digitales iniciales se establece entre una Pasarela de Medios y un Controlador de Pasarela de Medios. La clave S de la Pasarela de Medios y del Controlador de Pasarela de Medios puede ser diferente si únicamente puede validar la firma digital de la otra. Un campo/paquete de un protocolo de MEGACO expandido puede usarse para transmitir la clave y el parámetro.

Una señalización de registro se inicia desde una Pasarela de Medios a un Controlador de Pasarela de Medios para registro, en el que la señalización de registro tiene un parámetro para generar una clave compartida y una firma digital. Una clave compartida se genera después de que el Controlador de Pasarela de Medios ha validado la Pasarela de Medios. Un comando de modificación se inicia desde el Controlador de Pasarela de Medios a la Pasarela de Medios, en el que el comando de modificación tiene un parámetro para generar una clave compartida, una firma digital y un tiempo de vida de una clave compartida. Una clave compartida se genera después de que la Pasarela de Medios ha validado el Controlador de Pasarela de Medios.

En cada llamada y cada respuesta posteriores entre la Pasarela de Medios y el Controlador de Pasarela de Medios, las firmas se adjuntan a cada llamada y a cada respuesta entre la Pasarela de Medios y el Controlador de Pasarela de Medios usando la clave compartida. Si son válidas después de validarse entre sí, se establece un servicio de llamada, de otra manera la llamada se deniega.

Después de que ha expirado el tiempo de vida de la clave compartida, el Controlador de Pasarela de Medios hace a la clave inicial inválida, y la Pasarela de Medios pide al Controlador de Pasarela de Medios usando un comando de notificación generar una nueva clave compartida y obtener un tiempo de vida de una nueva clave.

La clave por lo tanto se actualiza periódicamente, y las llamadas se autentican mediante una nueva clave.

Una realización de la presente invención se ilustrará a continuación haciendo referencia a los dibujos.

La Figura 2 es un diagrama de flujo que muestra un método de autenticación para la Pasarela de Medios de la presente invención. Una clave inicial S se establece entre una Pasarela de Medios y un Controlador de Pasarela de Medios.

201) Un mensaje de registro se inicia desde una Pasarela de Medios a un Controlador de Pasarela de Medios, en el que el mensaje de registro tiene un parámetro M para generar una clave compartida mediante el Controlador de Pasarela de Medios y una firma digital generada mediante la clave S para el parámetro M de la clave compartida o el mensaje de registro.

202) La firma digital se valida usando la clave S después de que el Controlador de Pasarela de Medios recibe el mensaje. Si es válida, se genera una clave compartida S' usando el parámetro M de la clave compartida, y se envía una respuesta a la Pasarela de Medios.

203) Un mensaje de modificación se inicia desde el Controlador de Pasarela de Medios a la Pasarela de Medios, en el que el mensaje de modificación tiene un parámetro N para generar una clave compartida mediante la Pasarela de Medios y una firma digital generada mediante la clave S para el parámetro N de la clave compartida o el mensaje completo, y tiene también un tiempo de vida de una nueva clave compartida en la que el tiempo de vida es el tiempo, o el número de veces que puede usarse la nueva clave compartida para autenticación.

204) La firma digital se valida usando la clave S después de que la Pasarela de Medios recibe el mensaje. Si es válida, se genera una clave compartida S' usando el parámetro M de la clave compartida, y se envía una respuesta al Controlador de Pasarela de Medios.

205) En un mensaje (tal como AÑADIR (ADD)) establecido en cada llamada posterior, se adjunta una firma digital mediante el Controlador de Pasarela de Medios usando una nueva clave compartida S'.

206) La firma digital se valida usando la nueva clave compartida S' después de que la Pasarela de Medios recibe el mensaje. Si es válida, el Controlador de Pasarela de Medios es válido. Para una respuesta del Controlador de Pasarela de Medios, se adjunta también una firma digital usando la nueva clave compartida S'. La firma digital se valida usando la nueva clave compartida S' después de que el Controlador de Pasarela de Medios la recibe. Si es válida, se establece una llamada, de otra manera, la Pasarela de Medios es inválida y la llamada se deniega. El mismo método se usa para la autenticación periódica entre la Pasarela de Medios y el Controlador de Pasarela de Medios.

207) Después de que el tiempo de vida de la clave compartida establecido mediante el Controlador de Pasarela de Medios ha expirado, se envía un mensaje de notificación desde la Pasarela de Medios al Controlador de Pasarela de Medios, en el que el mensaje de notificación tiene un parámetro M' para generar una clave compartida mediante el Controlador de Pasarela de Medios y una firma digital generada mediante la clave S para el parámetro M' de la clave compartida o del mensaje completo.

208) La firma digital se valida usando la clave S después de que el Controlador de Pasarela de Medios recibe el mensaje. Si es válida, se genera una clave compartida S'' usando el parámetro M' de la clave compartida, y se envía una respuesta a la Pasarela de Medios.

209) Un mensaje de modificación se inicia desde el Controlador de Pasarela de Medios a la Pasarela de Medios, en el que el mensaje de modificación tiene un parámetro N' para generar una clave compartida mediante la Pasarela de Medios y una firma digital generada mediante la clave S para el parámetro N' de la clave compartida o del mensaje completo, y tiene también un tiempo de vida de una nueva clave compartida. Una nueva clave compartida S'' se genera usando el parámetro N' de la clave compartida mediante la Pasarela de Medios, y las llamadas posteriores se autentican y se autentican periódicamente usando la nueva clave compartida S''.

210) Una respuesta se envía desde la Pasarela de Medios al Controlador de Pasarela de Medios.

Después de que el tiempo de vida de la nueva clave compartida S'' ha expirado, se genera una nueva clave compartida S'' repitiendo las etapas 207)-210), y así sucesivamente.

Aunque el método de autenticación para la Pasarela de Medios usando el protocolo de MEGACO se ha descrito particularmente con respecto a la realización del mismo, se entenderá por los expertos en la materia que pueden realizarse muchas modificaciones y cambios en formas y detalles sin alejarse del alcance y espíritu de la presente invención. Por ejemplo, debido a la similitud del protocolo de MEGACO y el protocolo de MGCP, la solución técnica de la presente invención es apropiada también para la Pasarela de Medios usando el protocolo de MGCP. Por lo tanto, las realizaciones anteriormente descritas pretenden ilustrar pero no limitar, y muchas modificaciones y cambios pueden caer dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método de autenticación para Pasarela de Medios, **caracterizado por que** el método comprende:

establecer una clave inicial para validar firmas digitales iniciales entre una Pasarela de Medios y un Controlador de Pasarela de Medios;
generar una nueva clave compartida que tiene un tiempo de vida específico realizando comunicación de señalización entre dicha Pasarela de Medios y dicho Controlador de Pasarela de Medios con dicha clave inicial;
autenticar llamadas y respuestas entre dicha Pasarela de Medios y dicho Controlador de Pasarela de Medios con dicha nueva clave compartida; y
actualizar dicha clave compartida entre dicha Pasarela de Medios y dicho Controlador de Pasarela de Medios si el tiempo de vida de dicha clave compartida ha expirado.

2. El método de acuerdo con la reivindicación 1, **caracterizado por que** la etapa de generación de una nueva clave compartida comprende adicionalmente:

iniciar una señalización de registro desde dicha Pasarela de Medios a dicho Controlador de Pasarela de Medios para registro, en el que dicha señalización de registro tiene un parámetro para generar una clave compartida y una firma digital generada mediante dicha clave inicial;
generar una clave compartida y establecer un tiempo de vida de dicha clave compartida después de que dicho Controlador de Pasarela de Medios ha validado dicha Pasarela de Medios con dicha clave inicial;
iniciar un comando de modificación desde dicho Controlador de Pasarela de Medios a dicha Pasarela de Medios, en el que dicho comando de modificación tiene un parámetro para generar la clave compartida, una firma digital generada mediante dicha clave inicial y un tiempo de vida de una clave compartida; y
generar la clave compartida y establecer el tiempo de vida de dicha clave compartida después de que dicha Pasarela de Medios ha validado dicho Controlador de Pasarela de Medios con dicha clave inicial;

3. El método de acuerdo con la reivindicación 1, **caracterizado por que** la etapa de autenticación comprende adicionalmente:

para cada llamada, adjuntar una firma digital a cada mensaje de llamada desde dicho Controlador de Pasarela de Medios a dicha Pasarela de Medios usando dicha clave compartida;
validar dicha firma digital en dicho mensaje de llamada en dicha Pasarela de Medios usando dicha clave compartida, y si es válida, devolver un mensaje de respuesta adjunto con una firma digital usando dicha clave compartida a dicho Controlador de Pasarela de Medios; y
validar dicha firma digital en dicho mensaje de respuesta en dicho Controlador de Pasarela de Medios usando dicha clave compartida, si es válida, establecer un servicio de llamada, de otra manera denegar la llamada.

4. El método de acuerdo con la reivindicación 1, **caracterizado por que** la etapa de actualización de dicha clave compartida comprende adicionalmente:

enviar un comando de notificación desde dicha Pasarela de Medios a dicho Controlador de Pasarela de Medios, pidiendo a dicho Controlador de Pasarela de Medios generar una nueva clave compartida, en el que dicho comando de notificación tiene un parámetro para generar una clave compartida y una firma digital generada mediante una clave inicial;
generar una nueva clave compartida y establecer un tiempo de vida de dicha clave compartida después de que dicho Controlador de Pasarela de Medios ha validado dicha Pasarela de Medios con dicha clave inicial;
iniciar un comando de modificación desde dicho Controlador de Pasarela de Medios a dicha Pasarela de Medios, en el que dicho comando de modificación tiene un parámetro para generar la clave compartida, una firma digital generada mediante dicha clave inicial y el tiempo de vida de la clave compartida; y
generar la clave compartida y establecer el tiempo de vida de dicha clave compartida después de que dicha Pasarela de Medios ha validado dicho Controlador de Pasarela de Medios con dicha clave inicial.

5. El método de acuerdo con la reivindicación 2, 3 o 4, **caracterizado por que** el algoritmo usado para generar una clave compartida mediante dicho Controlador de Pasarela de Medios y dicha Pasarela de Medios es diferente del algoritmo usado para generar una firma digital mediante dicho Controlador de Pasarela de Medios y dicha Pasarela de Medios.

6. El método de acuerdo con la reivindicación 2, 3 o 4, **caracterizado por que** se usa un campo/paquete de un protocolo expandido para transmitir dicho parámetro para generar una clave compartida y dicha firma digital.

7. El método de acuerdo con la reivindicación 1, **caracterizado por que** el tiempo de vida de dicha clave compartida es el tiempo, o el número de veces que puede usarse dicha clave compartida para autenticación.

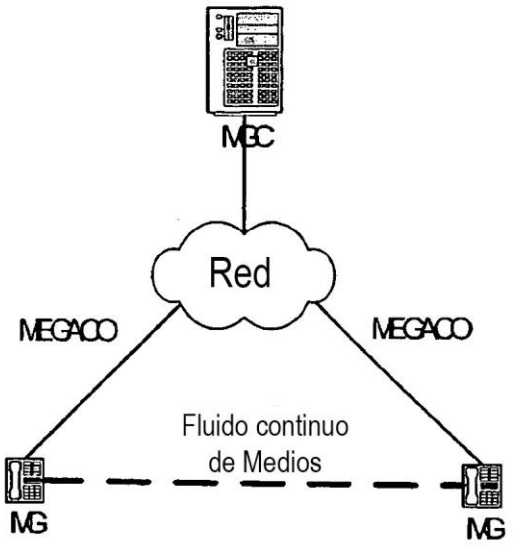
MGC
Red
MEGACO
MEGACO
Fluido continuo
de Medios
MG
MG

Fig. 1

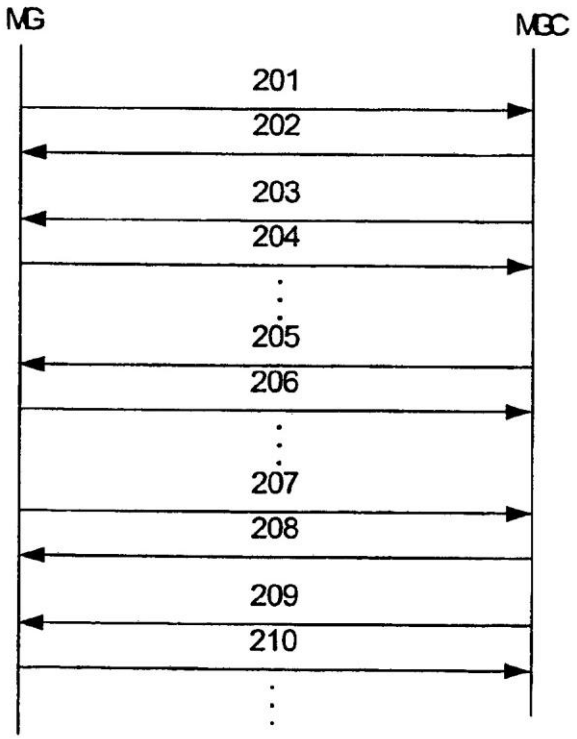
MG
MGC
201
202
203
204
205
206
207
208
209
210

Fig. 2