(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 604 579**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04W 12/04 (2009.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.01.2002 PCT/US2002/01830**

(87) Fecha y número de publicación internacional: **06.09.2002 WO02069605**

(96) Fecha de presentación y número de la solicitud europea: **24.01.2002 E 02701075 (0)**

(97) Fecha y número de publicación de la concesión europea: **26.10.2016 EP 1371206**

(54) Título: **Método y sistema para delegación de procedimientos de seguridad a un dominio visitado**

(30) Prioridad:

21.02.2001 US 269956 P
23.11.2001 US 990329

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.03.2017

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

FACCIN, STEFANO y
LE, FRANCK

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método y sistema para delegación de procedimientos de seguridad a un dominio visitado

Campo técnico

Esta invención se refiere a hacer itinerancia en nodos móviles en un dominio visitado, y más específicamente a delegar procedimientos de seguridad, tales como autenticación y distribución de clave, al dominio visitado.

Antecedentes de la técnica

Los dispositivos móviles tales como teléfonos celulares, Asistentes Digitales Personales (PDA), ordenadores portátiles, etc., son abundantes en la sociedad de hoy en día. Un gran número de personas llevan teléfonos móviles diariamente mientras viajan del hogar al trabajo y a otros lugares durante el día. En la mayoría de los casos, el dispositivo móvil tiene una suscripción con un dominio doméstico. Este dominio doméstico mantiene información acerca del usuario tal como la clave a largo plazo para procedimientos de seguridad pero también información con respecto a los servicios que se ha suscrito el usuario y por lo tanto está autorizado a tener acceso, etc.

Cuando un dispositivo/nodo móvil hace itinerancia a un dominio externo (es decir, dominio visitado), el usuario del nodo móvil necesita estar autorizado por el dominio externo para obtener acceso a recursos locales del dominio visitado. La autorización generalmente consiste en ofrecer el usuario sus credenciales a un agente local (por ejemplo, un cliente de Autenticación, Autorización y Contabilidad (AAA) local) para verificar que el usuario está autorizado (por ejemplo, mediante acuerdo de itinerancia entre el dominio doméstico y el dominio visitado (por ejemplo, Proveedores de Servicio de Internet (ISP))) y para autenticar el usuario.

Además, cuando un usuario/nodo móvil está haciendo itinerancia, normalmente necesitan establecerse muchas asociaciones de seguridad (SA) entre el usuario y los agentes o entidades del dominio visitado. Por ejemplo, puede ser necesaria una asociación de seguridad entre el usuario y el encaminador de acceso en un dominio visitado para proteger datos (protección de confidencialidad e integridad) a través del enlace de acceso. Como otro ejemplo, en el contexto del Protocolo de Internet Móvil (MIP), puede ser necesaria una SA entre el nodo móvil (MN) y el agente doméstico cuando esta se asigna en el dominio visitado. Como un tercer ejemplo, puede requerirse también una asociación de seguridad entre el nodo móvil y agentes de movilidad cuando se despliega una solución de Gestión de Movilidad Localizada. Estas asociaciones de seguridad normalmente tienen un tiempo de vida restringido, y cuando expiran, necesitan refrescarse. Además, para evitar fraude, los proveedores de servicio necesitan la capacidad de forzar a un usuario para que proporcione información de autenticación en cualquier momento durante una sesión. Tanto el proveedor de servicio de dominio doméstico como el proveedor de servicio del dominio visitado necesitan tener esta capacidad.

Además, para conseguir mejor seguridad global, un nodo móvil puede desear desafiar la red en cualquier momento, por ejemplo para evitar ataques de suplantación de red, ataques de hombre en el medio, etc. Todos estos procedimientos requieren la implicación del servidor de AAA doméstico (AAAh), puesto que únicamente el usuario/nodo móvil y su dominio doméstico comparten una clave a largo plazo. Esto implica que son necesarios varios viajes de ida y vuelta de mensaje entre un dominio visitado y un dominio doméstico para soportar la autorización/autenticación y los procedimientos de distribución de clave anteriormente mencionados. Estos intercambios de mensajes entre la red de dominio doméstico y la red de dominio visitado pueden crear una carga de señalización excesiva entre el AAAh y el servidor de AAA visitado (AAAv) y pueden añadir también retardo en el procedimiento.

El documento EP-A-0673178, 20 de septiembre de 1995, (20-09-1995), desvela un método de autenticación de desafío-respuesta para comunicaciones móviles.

Por lo tanto, existe una necesidad para un método y aparato que permitan al usuario/nodo móvil y a una red visitada realizar procedimientos de autenticación y de distribución de clave sin requerir muchas comunicaciones de ida y vuelta entre la red visitada y la red de dominio doméstico del usuario, y que proporcione una asociación de seguridad local (LSA) que permita optimizaciones y capacite a una red visitada autenticar un usuario en cualquier momento, así como capacite al usuario autenticar la red en cualquier momento, y realice los procedimientos de distribución de clave sin la implicación del dominio doméstico, mientras mantenga aún un buen nivel de seguridad.

Divulgación de la invención

La presente invención se refiere a un método para delegación de procedimientos de seguridad a un segundo dominio. Se genera una primera clave para un nodo móvil. La primera clave se almacena en el nodo móvil y en un dominio doméstico del nodo móvil. El nodo móvil se mueve al segundo dominio. Se envía una solicitud desde el segundo dominio al dominio doméstico para autenticar el nodo móvil. Se genera una segunda clave en el dominio doméstico usando la primera clave y un número aleatorio y el número aleatorio y la segunda clave se envían al segundo dominio. El número aleatorio se envía al nodo móvil por el segundo dominio. El nodo móvil genera la

segunda clave usando el número aleatorio y la primera clave. La segunda clave se usa para al menos un procedimiento de autenticación entre el nodo móvil y el segundo dominio.

Una solicitud de autenticación de red puede generarse por el nodo móvil y enviarse al segundo dominio. El segundo dominio puede generar una primera respuesta de autenticación usando la tercera clave y la solicitud de autenticación de red. La respuesta de autenticación de red puede enviarse al nodo móvil. El nodo móvil puede generar la tercera clave usando la primera clave y el segundo número aleatorio. El nodo móvil puede generar una segunda respuesta de autenticación usando la tercera clave y la solicitud de autenticación de red. La primera respuesta de autenticación generada por el segundo dominio y la segunda respuesta de autenticación generada por el nodo móvil pueden compararse. El nodo móvil puede autenticar el segundo dominio si se compara la segunda respuesta de autenticación y la primera respuesta de autenticación. El segundo dominio puede notificarse de que la segunda clave se ha actualizado con la tercera clave si se compara la primera respuesta de autenticación y la segunda respuesta de autenticación. El segundo dominio puede usar la tercera clave para los procedimientos de autenticación entre el nodo móvil y el segundo dominio.

El segundo dominio puede generar un tercer número aleatorio y enviar el tercer número aleatorio al nodo móvil. El nodo móvil puede generar segundos datos de autenticación usando el tercer número aleatorio y la tercera clave. Los segundos datos de autenticación pueden enviarse al segundo dominio. El segundo dominio puede usar los segundos datos de autenticación para verificar que el nodo móvil ha actualizado la segunda clave con la tercera clave.

La presente invención se refiere también a un método para delegación de procedimientos de seguridad a un segundo dominio donde se comparte una primera clave con un nodo móvil y al menos un servidor en el dominio doméstico del nodo móvil. El nodo móvil se mueve en el segundo dominio. Se solicita la autenticación del nodo móvil por el dominio doméstico. Se genera una segunda clave usando la primera clave en el dominio doméstico. La segunda clave se envía al segundo dominio. La segunda clave se usa para al menos un procedimiento de autenticación entre el nodo móvil y el segundo dominio.

Además, la presente invención se refiere a un sistema para delegación de procedimientos de seguridad a un segundo dominio. El sistema incluye un dominio doméstico, un dispositivo móvil, y el segundo dominio. El dominio doméstico contiene al menos un servidor. El dispositivo móvil comparte una primera clave con al menos un servidor en el dominio doméstico. El segundo dominio contiene al menos un segundo servidor. Existe una asociación de seguridad entre el al menos un servidor en el dominio doméstico y al menos un segundo servidor en el segundo dominio. Cuando el dispositivo móvil hace itinerancia en el segundo dominio, el segundo dominio solicita autenticación del dispositivo móvil por el dominio doméstico. El al menos un servidor genera una segunda clave usando la primera clave y envía la segunda clave al segundo dominio. La segunda clave se usa para al menos un procedimiento de autenticación entre el dispositivo móvil y el segundo dominio. El segundo dominio puede ser un dominio visitado.

La presente invención se refiere adicionalmente a un método para delegación de procedimientos de seguridad a un segundo dominio que incluye mover un dispositivo móvil al segundo dominio donde el nodo móvil tiene un dominio doméstico. Una segunda clave se envía desde el dominio doméstico al segundo dominio para autenticación del dispositivo móvil. La segunda clave está basada en una primera clave compartida entre el dominio doméstico y el dispositivo móvil. El segundo dominio autentica el dispositivo móvil usando la segunda clave. La segunda clave se usa para al menos un procedimiento de autenticación entre el dispositivo móvil y el segundo dominio.

Breve descripción de los dibujos

La presente invención se describe adicionalmente en la descripción detallada que sigue en referencia a la pluralidad indicada de dibujos por medio de ejemplos no limitantes de realizaciones de la presente invención en las que números de referencia similares representan partes similares a lo largo de todas las varias vistas de los dibujos y en los que:

la Figura 1 es un diagrama de dominios con un nodo móvil en su dominio doméstico de acuerdo con una realización de ejemplo de la presente invención;
la Figura 2 es un diagrama de bloques de un modelo de seguridad de clave compartida temporal de acuerdo con una realización de ejemplo de la presente invención;
la Figura 3 es un diagrama de flujo de un proceso para creación y distribución de una clave compartida temporal de acuerdo con una realización de ejemplo de la presente invención;
la Figura 4 es un diagrama de flujo de mensajes durante generación y distribución de TSK cuando tiene lugar una autenticación mutua de acuerdo con una realización de ejemplo de la presente invención; y
la Figura 5 es un diagrama de flujo de un proceso de actualización de TSK de acuerdo con una realización de ejemplo de la presente invención.

Mejor modo para llevar a cabo la invención

Los detalles particulares mostrados en el presente documento son a modo de ejemplo y para fines de análisis ilustrativo de las realizaciones de la presente invención. La descripción tomada con los dibujos hace evidente para los expertos en la materia cómo puede realizarse la presente invención en la práctica.

Además, pueden mostrarse disposiciones en forma de diagrama de bloques para evitar oscurecer la invención, y también en vista del hecho de que los detalles específicos con respecto a una implementación de tales disposiciones de diagramas de bloques son altamente dependientes de la plataforma dentro de la que se ha de implementar la presente invención, es decir, los detalles específicos deberían estar de manera adecuada dentro del ámbito del experto en la materia. Cuando los detalles específicos (por ejemplo, circuitos, diagramas de flujo) se exponen para describir realizaciones de ejemplo de la invención, debería ser evidente para un experto en la materia que la invención puede ponerse en práctica sin estos detalles específicos. Finalmente, debería ser evidente que puede usarse cualquier combinación de circuitería de cableado permanente e instrucciones de software para implementar las realizaciones de la presente invención, es decir, la presente invención no está limitada a ninguna combinación específica de circuitería de hardware e instrucciones de software.

Aunque las realizaciones de ejemplo de la presente invención pueden describirse usando un diagrama de bloques de sistema de ejemplo en un entorno de unidad de anfitrión de ejemplo, la práctica de la invención no está limitada a lo mismo, es decir, la invención puede ponerse en práctica con otros tipos de sistemas, y en otros tipos de entornos:

> la referencia en la memoria descriptiva a “una realización” significa que un rasgo, estructura o característica particular descrita en relación con la realización se incluye en al menos una realización de la invención. Las apariciones de la frase “en una realización” en diversos lugares en la memoria descriptiva no son todas necesariamente haciendo referencia a la misma realización.

La presente invención se refiere a métodos y aparatos para autenticación de nodos móviles y redes, así como distribución de clave sin implicar la red doméstica que se refiere a establecer una asociación de seguridad local (LSA) entre un usuario (es decir, nodo móvil) y un dominio/red visitada cuando el usuario/nodo móvil ha hecho itinerancia desde su dominio doméstico al dominio visitado. Puede usarse una clave compartida a largo plazo entre un nodo móvil y su dominio doméstico para generar una clave compartida temporal (TSK) que puede usarse a continuación para fines de autenticación y generación de clave entre el dominio visitado y el nodo móvil sin ninguna implicación adicional del dominio doméstico. El término “usuario” y la expresión “nodo móvil” pueden usarse de manera intercambiable al ilustrar la presente invención y hacen referencia al dispositivo que comparte la clave a largo plazo con el dominio doméstico.

Por lo tanto, de acuerdo con la presente invención, una vez que se establece una TSK entre un usuario y un dominio visitado (con la implicación del dominio doméstico), pueden delegarse funciones tales como autenticación de entidad y derivación de clave al dominio visitado. Estas funciones se realizan de manera segura puesto que la clave compartida temporal específica de usuario se creó bajo el control del dominio doméstico y se distribuyó de manera segura al dominio visitado y al usuario/nodo móvil. Por lo tanto, el dominio doméstico no necesita implicarse en ningún procedimiento de autenticación o derivación de clave futuro que implique al dominio visitado y al nodo móvil.

La Figura 1 muestra un diagrama de dominios con un nodo móvil en su dominio doméstico de acuerdo con una realización de ejemplo de la presente invención. La Figura 1 muestra teres dominios 10, 20 y 40. Cada dominio representa una red específica operada por un Proveedor de Servicio de Internet (ISP). Por ejemplo, el dominio 10 puede operarse por el ISP 1, el dominio 20 puede operarse por el ISP 2, y el dominio 40 puede operarse por el ISP 4. Cada dominio 10, 20, 40 puede incluir una infraestructura de Autenticación, Autorización y Contabilidad (AAA) compuesta de servidores de AAA y clientes de AAA (12, 22 y 42). Cada dominio puede incluir también uno u otros más nodos o entidades de red que pueden realizar diversas funciones en el dominio. El dominio 10 incluye las entidades 14-18, el dominio 20 incluye las entidades 24-28, y el dominio 40 incluye las entidades 44 y 46. Estas entidades pueden ser servidores, encaminadores, clientes, agentes, etc. Pueden haber múltiples usuarios con dispositivos móviles (es decir, nodos móviles), basados en cada dominio particular. Por ejemplo, el nodo móvil 30 tiene su dominio doméstico como el dominio 10. Un servidor de AAA en un dominio puede tener un canal seguro con servidores de AAA en otros dominios. El servidor de AAA 12 en el dominio 10 tiene una asociación de seguridad 50 con el servidor de AAA 22 en el dominio 20. La asociación de seguridad 50 permite que exista un canal seguro para comunicación de información sensible. La asociación de seguridad 50 puede usarse para transmitir claves y otra información a través de una interfaz segura. Si el usuario/nodo móvil 30 se mueve desde el domino 10 al dominio 20 (usuario/nodo móvil 30 mostrados en líneas discontinúas en el domino 20), el servidor de AAA 22 puede usar la asociación de seguridad 50 para entrar en contacto con el servidor de AAA 12 para autenticar el nodo móvil 30 en el dominio visitado 20.

La Figura 2 muestra un diagrama de bloques de un modelo de seguridad de clave compartida temporal de acuerdo con una realización de ejemplo de la presente invención. Un cliente AAA (AAAc) 26 puede realizar una función que permite a un usuario 30 autenticarse y autorizarse por un proveedor de servicio de red visitada para obtener acceso a conductividad de IP en el dominio visitado 20. El usuario 30 proporciona su identidad y datos de autenticación al

AAAc 26 en la red visitada 20, que a continuación puede usar una infraestructura AAA para autenticar y autorizar al usuario 30 para uso de los recursos de dominio visitado, y eventualmente transportar otra información. Los detalles específicos del intercambio entre un usuario/nodo móvil y un AAAc de datos de autenticación (por ejemplo, tipo de datos, número de intercambios, etc.) pueden basarse en el algoritmo de autenticación específico adoptado entre los dos. Un AAAc puede ser cualquiera de muchos tipos de entidades, por ejemplo, un asistente (por ejemplo, localizado en el encaminador por defecto o encaminador de acceso (el primer encaminador visible para el usuario en la red visitada)), el agente de registro del dominio visitado, o puede ser cualquier servidor en la red visitada. La presente invención puede aplicarse a todos estos casos. Por motivos de ilustración de la presente invención, esta entidad se denominará como un AAAc por motivos de generalidad.

Una infraestructura de AAA de acuerdo con la presente invención puede basarse en una red de entidades de AAA. AAAc representa un cliente de AAA en una red visitada 20, AAAv, representa un servidor de AAA en el dominio visitado 20 mientras que AAAh representa un servidor de AAA en la red doméstica 10 del nodo móvil 30. Puede usarse un número de protocolos que localizan un agente 28 (entidad de par) en un dominio visitado para entregar paquetes de datos, o intercambiar mensajes de señalización específicos de protocolo, con el nodo móvil 30. IP móvil, radiobúsqueda de IP, y SIP (Protocolo de Internet Simple) son ejemplos de tales protocolos. Cualquiera de estos protocolos puede tener un requisito o una recomendación para tener una clave de seguridad entre un nodo móvil 30 y un agente 28. La clave de seguridad puede usarse para autenticar y/o encriptar mensajes de señalización intercambiados entre el agente 28 y el nodo móvil 30. Esta clave compartida entre el nodo móvil 30 y el agente de cada protocolo en el dominio visitado 20 normalmente no puede preestablecerse sino que necesita establecerse dinámicamente. La autenticación puede requerirse antes de que se realice la distribución de clave.

El modelo de seguridad mostrado en la Figura 2 puede basarse en un conjunto de asociaciones de seguridad (SA) entre las entidades en el modelo. Algunas de las asociaciones de seguridad están preestablecidas. Por ejemplo, si se supone que el dominio doméstico y el dominio visitado comparten una asociación de seguridad (SA1) a largo plazo que no es específica a ningún usuario/nodo móvil particular y que puede establecerse automáticamente o establecerse fuera de línea como resultado de un acuerdo de itinerancia entre los dos dominios/redes 10 y 20. Puede adoptarse cualquier mecanismo para establecer tales asociaciones de seguridad y aún estará dentro del espíritu y alcance de la presente invención. De acuerdo con la presente invención, se supone en particular que existe SA1 entre AAAh y AAAv. Esta asociación de seguridad puede usarse para intercambiar información de una forma segura y mutuamente autenticada en las dos redes 10, 20 por los servidores de AAA.

Además, de acuerdo con la presente invención, se supone que cada red 10, 20 tiene su propio mecanismo de seguridad y asociaciones de seguridad (SA2 y SA4) que permiten a las entidades en la misma red comunicar de una manera segura y mutuamente autenticada (por ejemplo, usando seguridad de IP (IPSEC) y una Infraestructura de Clave Pública (PKI) local). Además, de acuerdo con la presente invención, se supone que cada usuario/nodo móvil, como un resultado de un acuerdo de suscripción con un dominio doméstico, tiene una asociación de seguridad a largo plazo (SA3) (no mostrada) con el dominio doméstico del usuario. Tal asociación de seguridad permite la autenticación mutua entre el nodo móvil y el dominio doméstico. De acuerdo con la presente invención, se supone en particular, que un nodo móvil y un servidor doméstico de AAA comparten un conjunto común de algoritmos y un conjunto común de claves. Estos algoritmos y claves pueden usarse para autenticar el usuario al dominio doméstico y el dominio doméstico al usuario. En el caso donde estén disponibles múltiples algoritmos, puede necesitarse que tenga lugar una negociación entre el usuario y el servidor de AAAh para seleccionar un algoritmo cuando se autentica al usuario y se establece/refresca la clave compartida temporal. SA3 puede usarse también para derivar otras asociaciones de seguridad dinámicas.

De acuerdo con la presente invención, un nodo móvil y un dominio visitado tienen un conjunto de algoritmos de seguridad comunes que pueden usarse para soportar la adopción de una asociación de seguridad local entre ellos. Una asociación de seguridad local puede no ser posible si el nodo móvil y el dominio visitado no tienen un algoritmo en común. Estos algoritmos pueden necesitarse para autenticación mutua entre un usuario y el dominio visitado, si se requiere tal característica de cifrado y protección de integridad de mensajes entre el usuario y un agente en el dominio visitado, o la distribución de claves dinámicas entre el usuario y agentes en el dominio visitado basándose en la asociación de seguridad local. Un único algoritmo puede usarse para todas estas funciones, o un algoritmo diferente para cada una. Por lo tanto, debería estar disponible al menos un algoritmo común para el usuario y el dominio visitado. La negociación entre el nodo móvil y el dominio visitado puede ser necesaria para determinar si existe un algoritmo común y cuál es este algoritmo. Por ejemplo, MD5 puede ser el algoritmo común por defecto usado tanto para autenticación como establecimiento de claves dinámicas por un nodo móvil y dominio visitado.

Una vez que se establece una clave compartida temporal entre un usuario y un dominio visitado, con la implicación del dominio doméstico del usuario, la clave compartida temporal puede usarse para: autenticación del usuario por el dominio visitado en cualquier momento, autenticación del dominio visitado por el usuario en cualquier momento, o control por el dominio visitado de la distribución de clave entre el usuario y agentes/entidades en el dominio visitado. Por ejemplo, la clave compartida temporal puede usarse para establecer una clave de seguridad entre el usuario y un agente en el dominio visitado (por ejemplo, encaminador de acceso) para proteger los datos (por ejemplo, encriptación y protección de integridad) intercambiados a través del enlace de acceso.

Además, la clave compartida temporal puede usarse para establecer una clave de seguridad entre un usuario y agentes de movilidad en el dominio visitado. En el contexto de IP móvil, si se adopta un esquema de Gestión de Movilidad Local, la clave compartida temporal puede usarse para autenticar los mensajes de actualización de unión/acuse de recibo de unión.

Todas estas funciones pueden realizarse usando la clave compartida temporal y sin la implicación del dominio doméstico, mientras se realizan aún de manera segura puesto que la clave compartida temporal específica de usuario se crea bajo el control del dominio doméstico y se distribuye de manera segura al dominio visitado y al usuario. El nodo en el dominio visitado al que puede distribuirse la clave compartida temporal puede ser un servidor de AAAv, o un cliente de AAA (AAAc) tal como un agente de registro. Dependiendo de las capacidades y tipo del AAAc (por ejemplo, el AAAc puede ser un agente de registro de URP (RA) frente a un agente externo MIPv4), la clave compartida temporal puede proporcionarse al AAAv o al AAAc. Por lo tanto, dependiendo de dónde se distribuya la clave compartida temporal, los procedimientos de autenticación y de distribución de clave basándose en la clave compartida temporal pueden realizarse en diferentes entidades (por ejemplo, AAAv frente a AAAc) en el dominio visitado.

De acuerdo con la presente invención, una clave compartida temporal es una optimización para procedimientos de seguridad existentes cuando se considera la señalización implicada entre el dominio visitado y el doméstico. Sin embargo, si se usa una asociación de seguridad local (es decir, se proporciona una clave compartida temporal al dominio visitado) puede depender de políticas de la red doméstica y acuerdos de itinerancia. Por ejemplo, para maximizar la seguridad, puede haber casos en los que un dominio doméstico no esté dispuesto a compartir la clave compartida temporal con un dominio visitado. Esto puede tener lugar, por ejemplo, cuando el usuario se mueve a un dominio visitado que el dominio doméstico no confía suficientemente. La localización de un dominio visitado puede ser también una razón por la que un dominio doméstico no esté dispuesto a compartir la clave compartida temporal con el dominio visitado.

De acuerdo con la presente invención, pueden requerirse las extensiones del protocolo Diameter para soportar el mecanismo de clave compartida temporal. Los parámetros intercambiados por un usuario y el AAAc pueden llevarse a cabo de muchas maneras, por ejemplo, en opciones de destino de IPv6, en mensajes de ICMPv6, en mensajes de URP, por EAP, etc. Cualquier protocolo puede usarse para intercambiar esta información y aún estar dentro del espíritu y alcance de la presente invención.

Cuando un usuario se mueve a un nuevo dominio visitado y se registra en primer lugar, el servidor de AAAh del nodo móvil se invoca para verificar la validez del nodo móvil. Si las políticas del dominio visitado y del dominio doméstico permiten y sugieren el uso de la clave compartida temporal, pueden tener lugar ciertos procesos. Por ejemplo, el dominio doméstico puede generar una nueva clave compartida temporal si no se ha establecido y distribuido previamente la clave compartida temporal al dominio visitado. La clave compartida temporal puede actualizarse si la clave compartida temporal previamente establecida y distribuida al usuario y al dominio visitado ha expirado (por ejemplo, tiempo de vida limitado de TSK) o la clave compartida temporal se usó previamente en un dominio visitado diferente y por motivos de seguridad es la política del dominio doméstico generar una nueva clave compartida temporal.

Por lo tanto, la clave compartida temporal puede distribuirse al usuario y al dominio visitado en el caso donde se genere/actualice la clave compartida temporal, y en el caso donde se use un valor previo de una clave compartida temporal. En el último escenario, la clave compartida temporal únicamente necesita distribuirse al dominio visitado, puesto que el usuario ya la tiene. El usuario necesita estar informado de que la clave compartida temporal previa es aún válida.

Preferentemente, un AAAh actualiza la clave compartida temporal al menos cada vez que un nodo móvil entra en un nuevo dominio visitado, de otra manera, el dominio visitado previo tiene el valor de la clave compartida temporal y podría actuar en nombre del usuario/nodo móvil y llevar a cabo acciones indeseables. Las políticas de red pueden determinar si se sigue este proceso.

La Figura 3 muestra un diagrama de flujo de un proceso para la creación y distribución de una clave compartida temporal de acuerdo con una realización de ejemplo de la presente invención. Como se ha descrito anteriormente, se comparte una clave a largo plazo entre el nodo móvil y su dominio doméstico: por ejemplo se configura en el momento de la suscripción. La clave a largo plazo se almacena en el nodo móvil y en el dominio doméstico. Cuando el nodo móvil se mueve a un dominio visitado S1, el dominio visitado envía una solicitud al dominio doméstico del nodo móvil para autenticar el nodo móvil S2. Después de que el usuario está autenticado, y si los dominios doméstico y visitado deciden usar la clave compartida temporal, se genera una clave compartida temporal en el dominio doméstico usando la clave a largo plazo y un número aleatorio S3. El dominio doméstico puede usar también otra información junto con la clave a largo plazo para generar la clave compartida temporal. La clave compartida temporal y el número aleatorio (y posiblemente otra información) se envían al dominio visitado por el dominio doméstico S4. El número aleatorio se envía al nodo móvil por el dominio visitado S5. El nodo móvil genera la clave compartida temporal usando el número aleatorio y la clave a largo plazo S6. La TSK se usa para procedimientos de autenticación entre el nodo móvil y el dominio visitado S7.

La realización de ejemplo en la Figura 3 es solo una de muchas posibles maneras para generar y distribuir la clave compartida temporal al mismo tiempo que la red autentica el usuario y el usuario autentica la red. El procedimiento usado para crear la clave compartida temporal es independiente del mecanismo de autenticación usado para autenticar el usuario/nodo móvil. Pueden adoptarse diferentes tipos o protocolos de EAP para autenticación. El dominio visitado tiene la clave compartida temporal y puede usar la clave compartida temporal en cualquier manera que vea que se ajusta para autenticar el nodo móvil.

La Figura 4 describe en más detalle cómo se combina la generación y distribución de TSK con la autenticación de usuario/red cuando el usuario se registra en primer lugar en el dominio visitado y cuando el mecanismo de autenticación está basado en desafío-respuesta. En esta realización de ejemplo, el dominio visitado difunde un desafío local y el usuario usa este desafío local (LC), un identificador de red visitada (VN_ID), y la clave a largo plazo para calcular algún dato de autenticación (AUTHU). El usuario puede generar también un desafío de anfitrión (HC) para requerir autenticación de red. El usuario envía el ID de usuario (ID), (es decir, ID de nodo móvil), AUTHU, LC, y HC al cliente de AAA. El cliente de AAA a continuación reenvía esta información al AAAv incluyendo el desafío local el ID de la red visitada. El AAAv reenvía el mensaje o mensajes que contienen la información al AAAh. A partir del desafío local, el ID de la red visitada, y la clave a largo plazo compartida específica de usuario recuperada gracias al ID de usuario/nodo (por ejemplo, el Identificador de Acceso de Red), el AAAh verifica la validez del usuario. El AAAh a continuación calcula los datos de autenticación de red (AUTHNET) desde el desafío de anfitrión y la clave a largo plazo, y genera eventualmente algún material de clave si se solicita a los servidores de AAA desempeñar un papel en la distribución de clave. Si el AAAh y AAAv deciden usar la clave compartida temporal, el AAAh genera un nuevo número aleatorio (RANDTSK) y ejecuta el algoritmo compartido con el nodo móvil usando la clave a largo plazo (SA3) para calcular la nueva clave compartida temporal (TSK) “pendiente”. RANDTSK, TSK, AUTHNET, y HC se envían desde el AAAh al AAAv. El AAAv reenvía RANDTSK, AUTHNET, y HC al cliente de AAA, que a continuación reenvía esta información al nodo móvil.

TSK-AVP puede enviarse en cualquier código de comando ya definido tal como el comando Diameter-EAP-respuesta (DEA) o el comando AAA-nodo-móvil-respuesta (AMA). Este AVP llevará la TSK pendiente al dominio visitado (AAAv) y, por lo tanto, los mensajes deberían protegerse bajo la asociación de seguridad de AAA entre el AAAh y el AAAv. RANDTSK puede enviarse en un RANDTSK-AVP, de la misma manera que TSK-AVP, es decir, en cualquier código de comando ya definido tal como el comando Diameter-EAP-respuesta o el comando AAA-nodo-móvil-respuesta. El usuario usará RANDTSK para derivar la correspondiente TSK. El AAAc, por lo tanto, convierte RANDTSK-AVP al protocolo apropiado para enviar al usuario. RANDTSK puede enviarse al usuario en cualquier protocolo y estará dentro del espíritu y alcance de la presente invención, por ejemplo, en una opción de destino, mensaje de Protocolo de Mensaje de Control de Internet (ICMP)v6, protocolo de URP, etc.

El AAAh puede usar seguridad entre servidores de AAA para proteger el mensaje al AAAv. El nodo móvil verifica la autenticidad de la red gracias a los datos de autenticación de red (AUTHNET) calculados desde el desafío de anfitrión (HC). Si se proporciona RANDTSK al nodo móvil, el nodo móvil deriva, desde la clave a largo plazo y el algoritmo común compartido con su servidor de AAAh, la TSK correspondiente para usar para los posteriores procedimientos de autenticación de entidad y distribución de clave. El usuario recibe RANDTSK en el mensaje que lleva los datos de autenticación de red y puede estar seguro, por lo tanto, que la información está proviniendo desde su red doméstica.

La red doméstica debe poder actualizar la TSK en cualquier momento cuando el nodo móvil esté en un dominio visitado y la TSK esté compartida. Por ejemplo, la TSK puede corromperse y la red doméstica debe poder revocar la TSK realizando una nueva actualización de TSK. Una función de actualización de clave compartida temporal de acuerdo con la presente invención se refiere al proceso por el cual la TSK actual usada por un usuario en el dominio visitado se cambia a un nuevo valor bajo la dirección del AAAh. Este proceso se aplica también al escenario donde un usuario y un dominio visitado no comparten una TSK y es necesario que se genere una nueva TSK. Puede desearse que únicamente el AAAh pueda iniciar la actualización del valor actual de la TSK. El AAAh puede hacer esto en cualquier momento durante una sesión de acuerdo con las políticas de dominio doméstico.

En el lado de la red (es decir, lado del dominio visitado) puede ejecutarse un proceso de autenticación de usuario inmediatamente después de una actualización de TSK para confirmar que el usuario/nodo móvil objetivo ha cambiado satisfactoriamente su TSK. Este proceso puede tener lugar enviando la red visitada un desafío al nodo móvil. Basándose en los datos de autenticación recibidos esperados desde el nodo móvil (en respuesta al desafío) que deben ser a partir de usar la nueva TSK, la red visitada puede asegurar que la actualización de TSK ha sido satisfactoria y que el usuario tiene, y está usando, el nuevo valor de TSK. Esto asegura que el usuario puede autenticarse así mismo y la red visitada en el futuro.

En el lado del usuario (es decir, lado del nodo móvil) el usuario puede iniciar un procedimiento de autenticación de red cuando el usuario se dirige por una red visitada para cambiar el valor de TSK del usuario. Este procedimiento de autenticación permite al usuario autenticar la red visitada que emite la actualización de TSK, evitando por lo tanto que una red fraudulenta interrumpa la operación de red normal forzando la TSK del usuario a que se desalinee con la TSK de la red visitada legítima.

El AAAh puede iniciar un proceso de actualización de TSK en cualquier momento cuando el usuario/nodo móvil está en un dominio visitado y está compartiendo una TSK. La decisión sobre cuándo se actualiza la TSK puede basarse en las políticas de dominio doméstico. Preferentemente, la TSK no se cambia demasiado a menudo para que no desaparezcan de otra manera los beneficios de una TSK. Sin embargo, la TSK debe tener un tiempo de vida para asegurar que la misma TSK no se usa durante demasiado tiempo.

Para actualizar la TSK, el AAAh en primer lugar genera un número aleatorio RANDTSK; y a continuación ejecuta el algoritmo compartido con el usuario usando la clave a largo plazo y este número aleatorio para calcular la nueva Clave Compartida Temporal (TSK). El AAAh envía RANDTSK y la nueva TSK al AAAv en un RANDTSK-AVP y TSK-AVP, respectivamente. Estos AVP pueden enviarse en un código de comando ya definido tal como la solicitud de re-autenticación (Re-Auth-Request) (RAR). El AAAh puede a continuación esperar un informe desde el AAAv. Con el RANDTSK y la nueva TSK, el AAAv puede actualizar la TSK en el nodo móvil, responder a una solicitud de autenticación de red desde el nodo móvil, y verificar la actualización de la TSK emitiendo un procedimiento de autenticación específico de usuario al nodo móvil.

Tras recibir el RANDTSK y la nueva clave de TSK, el AAAv dirige el encaminador servidor para enviar una orden de actualización de clave de TSK, que incluye el RANDTSK, al nodo móvil. El nodo móvil puede responder con una solicitud de autenticación de red que incluye un desafío seleccionado por el nodo móvil. El AAAv ejecuta un algoritmo compartido usando como entradas el desafío del nodo móvil y la nueva TSK. El resultado del cálculo se envía al nodo móvil. Dependiendo si el parámetro equivale a los resultados correspondientes esperados, el nodo móvil indica una actualización de TSK satisfactoria o una insatisfactoria en un mensaje al AAAv. Si es satisfactoria, el sistema servidor (AAAv) ejecuta el procedimiento de autenticación específico de usuario: el sistema servidor desafía al usuario enviando el usuario un número generado aleatoriamente para autenticar el usuario y asegurar que el usuario ahora tiene el valor de TSK correcto. El usuario toma el número aleatorio y la TSK nuevamente derivada como entradas para un algoritmo compartido con el sistema servidor y calcula un parámetro de autenticación. El AAAv realiza las mismas etapas y por lo tanto verifica que el usuario ha actualizado el valor de TSK. De otra manera, el AAAv informa que el proceso de actualización de TSK ha fallado al AAAh.

La Figura 5 es un diagrama de flujo de un proceso de actualización de TSK de acuerdo con una realización de ejemplo de la presente invención. Se genera una nueva TSK en el dominio doméstico usando un nuevo número aleatorio (diferente del número aleatorio usado para generar la TSK inicial) y la clave a largo plazo. El nuevo número aleatorio, RANDTSK, y la nueva TSK se envían al dominio visitado. El dominio visitado envía el nuevo número aleatorio, RANDTSK, al nodo móvil. El nodo móvil, no conociendo si este proceso de actualización de TSK está proviniendo desde una red válida, genera un desafío de red, RANDNET, al dominio visitado. La red visitada genera una respuesta, AUTHNET, al desafío del nodo móvil usando la nueva TSK y el desafío, RANDNET, y envía la respuesta al nodo móvil. El nodo móvil genera la nueva TSK usando la clave a largo plazo y el nuevo número aleatorio RANDTSK. El nodo móvil a continuación calcula la nueva TSK y verifica la validez de la respuesta de autenticación de red AUTHNET basándose en la nueva TSK, y el RANDNET previamente generado. La respuesta generada por el nodo móvil se compara con la respuesta generada por la red visitada. Si estas dos respuestas no se comparan, el dominio visitado no se autentica y la nueva TSK no se usa por el nodo móvil. Si la respuesta se compara, el dominio visitado se ha autenticado y el nodo móvil actualiza la TSK actual con la nueva TSK. Dependiendo si AUTHNET equivale al resultado correspondiente esperado, la MN indica una actualización de TSK satisfactoria o una insatisfactoria en un mensaje al AAAv. Si es satisfactoria, el sistema servidor ejecuta el procedimiento de autenticación específico de usuario: desafía el usuario enviándole un número generado aleatoriamente RANDU para autenticarlo y asegurar que el usuario ahora tiene el valor de TSK correcto. El usuario toma RANDU y la TSK nuevamente derivada como entradas a un algoritmo compartido con el sistema servidor y calcula AUTHU. El AAAv realiza las mismas etapas y puede por lo tanto verificar que el usuario ha actualizado el valor de TSK. De otra manera el AAAv informa el fallo al AAAh.

Puede haber un caso donde un usuario/nodo móvil y su red doméstica ya tienen una clave compartida temporal establecida y desean reutilizar la TSK cuando entran en el dominio visitado. En este caso, la TSK necesita distribuirse a la red visitada (desde AAAh a AAAv). La TSK no necesita enviarse al usuario puesto que el usuario ya tiene conocimiento de ella. Sin embargo, aún necesita proporcionarse una indicación al usuario para informarle para que empiece a usar la TSK. Esto puede conseguirse estableciendo un valor específico en el campo RANDTSK enviado al usuario.

Una vez que se ha establecido una TSK entre un nodo móvil y un dominio visitado, esto posibilita que el dominio visitado realice autenticación de entidad (autenticación de usuario y autenticación de red) y distribución de clave sin implicar la red doméstica, reduciendo por lo tanto el retardo de tiempo y señalización entre los dos dominios. Sin una TSK, el algoritmo exacto usado para calcular los datos de autenticación depende de la asociación de seguridad entre el usuario y el AAAh. Los datos de autenticación se calculan normalmente usando la clave a largo plazo compartida entre el usuario y el AAAh, más alguna otra información y un algoritmo comúnmente compartido. Cuando se emplea el mecanismo de TSK, el usuario toma las mismas entradas, pero en lugar de usando la clave a largo plazo que comparte con su AAAh, el usuario usa la TSK que comparte con el AAAv y el algoritmo compartido. El sistema visitado, que tiene la TSK y el algoritmo compartido, puede a continuación autenticar el usuario sin invocar la red doméstica del usuario. La TSK puede usarse también por entidades en el dominio visitado para establecer

claves de sesión para usarse por las entidades y el usuario/nodo móvil.

El usuario puede desear autenticar la red y por lo tanto genera un número aleatorio, un desafío de anfitrión, para desafiar la red. En este caso, el usuario espera unos datos de autenticación de red calculados por el AAAh usando el desafío de anfitrión y actualmente, la clave compartida a largo plazo. El algoritmo exacto usado para calcular los datos de autenticación de red depende de la asociación de seguridad entre el usuario y el AAAh. Si se usa el mecanismo de TSK, el usuario envía el desafío de anfitrión para autenticar la red y el AAAv aplica el algoritmo común al desafío de anfitrión y la TSK para calcular los datos de autenticación, es decir, los datos de autenticación de red. La autenticación de red se proporciona por lo tanto sin implicar el AAAh.

Sin el uso de TSK, la distribución de clave entre un usuario y agentes en un dominio visitado puede basarse en la asociación de seguridad a largo plazo entre el usuario y su AAAh. Esta asociación de seguridad puede usarse para crear asociaciones de seguridad derivadas entre el nodo móvil y agentes en el dominio visitado.

Cuando se adopta la TSK, el usuario puede recibir la indicación de que la TSK se ha de usar y, por lo tanto, el usuario usa la TSK en lugar de la clave a largo plazo para calcular las claves derivadas. De esta manera, un AAAc/AAAv (dependiendo de a qué agente se proporcionó la TSK) usa la TSK también para la distribución de clave. Las claves pueden estar disponibles para el usuario y para AAAc/AAAv. El AAAh no necesita estar implicado en el procedimiento.

La distribución de clave puede basarse en números aleatorios donde el AAAc/AAAv genera el número aleatorio y lo combina con algunos otros datos, tales como por ejemplo la identidad del usuario o dirección de IP, para formar una entrada junto con la TSK a un algoritmo de derivación de clave. El número aleatorio puede transmitirse al usuario que realiza las mismas operaciones, y que tiene conocimiento de la TSK, terminando con la misma clave de sesión derivada. Pueden emplearse otros esquemas de distribución de clave y aún estar dentro del espíritu y alcance de la presente invención. Por ejemplo, el usuario y agente en el dominio visitado puede decidir establecer una clave basada en Diffie Hellman. Sin embargo, la principal vulnerabilidad de este mecanismo es la autenticación para evitar ataques de “hombre en el medio”. La TSK compartida entre el usuario y la red visitada puede proporcionar esta autenticación de valor Diffie Hellman.

Para implementar la presente invención, preferentemente se usan AVP de protocolo de parámetro específico. Estos AVP pueden ser extensiones a una Aplicación de Diameter actual tal como las extensiones NASREQ de Diameter, o al protocolo basado en Diameter o introducirse como parte de una nueva aplicación al protocolo Diameter Base. Una nueva aplicación de Diameter específica podría especificarse con sus propios códigos de comando para realizar procedimientos de actualización de TSK y todas las otras funciones de acuerdo con la presente invención. Tener una nueva aplicación al protocolo Diameter Base permite a los servidores de AAA identificar cuáles soportan el mecanismo de TSK. La presente invención identifica la información intercambiada a través de la interfaz, pero no es dependiente de ningún protocolo particular. La información puede llevarse mediante cualquier protocolo y estar dentro del espíritu y alcance de la presente invención, por ejemplo, como opciones de destino de IPv6, mensajes de ICMPv6 o cualquier otro método. Algunos AVP de protocolo Diameter de ejemplo que se usan preferentemente para implementar la presente invención incluyen: RANDTSK-AVP, TSK-AVP, RANDNET-AVP, AUTH-NET-AVP, RANDU-AVP, AUTHU-AVP, AAA-Informe-AVP, y AAA-Informe-ack-AVP.

RANDTSK-AVP puede ser de tipo cadena de octetos, y puede usarse para llevar el valor de RANDTSK desde el servidor de AAA al usuario en dos casos: (1) para indicar al cliente usar la TSK, y (2) para actualizar la TSK. Por lo tanto, este AVP puede usarse desde el AAAh al AAAv, y desde el AAAv al usuario del AAA. RANDTSK puede llevarse en un comando RAR, DEA o AMA. En el caso de un procedimiento de actualización de TSK, RANDTSK preferentemente debería enviarse en un comando RAR. Un valor específico bien definido, conocido a priori, del RANDTSK (TBD) permite que la red doméstica indique que el usuario empiece a usar el valor de TSK actual sin actualizarlo como se ha descrito anteriormente. Otro valor específico bien definido, conocido a priori, del RANDTSK (TBD) permite que la red doméstica indique que el usuario deje de usar la TSK actual.

TSK-AVP puede ser del tipo cadena de octetos. Puede usarse por el AAAh para indicar la utilización e informe del valor de la TSK al AAAv. TSK-AVP puede llevar el valor de clave compartida temporal y, por lo tanto, debe protegerse (P bit establecido a 1). Cuando el AAAh desea actualizar la TSK, envía también TSK-AVP al AAAv para informarle que realice un procedimiento de actualización de TSK. En tal caso, TSK-AVP puede llevar el valor de la nueva TSK. La TSK puede llevarse en un comando RAR, DEA o AMA. En el caso de un procedimiento de actualización de TSK, la TSK preferentemente se envía en un comando RAR.

RANDNET-AVP puede ser del tipo cadena de octetos. Puede llevar el desafío generado aleatoriamente por el usuario para autenticar la red. Este RANDNET-AVP puede enviarse, por lo tanto, desde el cliente de AAA al AAAv. Puede llevarse, por ejemplo, en un comando DER. En respuesta al AAAv debería calcular AUTHNET.

AUTHNET-AVP puede ser del tipo cadena de octetos. Puede llevar los datos de autenticación de red y enviarse en respuesta a un RANDNET. AUTHNET-AVP puede llevarse por lo tanto desde el AAAv al cliente AAA en un DEA o RAR.

RANDU-AVP puede ser de tipo cadena de octetos. Puede llevar el desafío generado aleatoriamente por el AAAv para autenticar el usuario y asegurar que el usuario ha actualizado la TSK. Este RANDU-AVP puede enviarse, por lo tanto, desde el AAAv al cliente AAA. Puede llevarse en un DEA o RAR, y en respuesta a que el usuario debiera calcular AUTHU.

AUTHU-AVP puede ser de tipo cadena de octetos. Puede llevar los datos de autenticación de usuario y enviarse en respuesta a un RANDU. AUTHU-AVP puede por lo tanto llevarse desde el cliente de AAA al AAAv en un comando DER.

AAA-Informe-AVP puede ser de tipo sin signo 32. Puede llevar el resultado (fallo/éxito) desde el AAAv al AAAh y puede enviarse, por lo tanto, en un comando DER.

AAA-Informe-ack-AVP puede ser de tipo sin signo 32. Este AVP puede enviarse desde el AAAh al AAAv y puede llevarse, por lo tanto, en un comando DEA.

Una clave compartida temporal de acuerdo con la presente invención es ventajosa en que posibilita a un sistema servidor realizar de manera segura funciones de autenticación de entidad y distribución de clave con el usuario/nodo móvil en nombre de la red doméstica, sin tener que implicar a la totalidad de la red. Esto ahorra viajes de ida y vuelta entre las redes visitada y doméstica y reduce el retardo de tiempo y carga de red. La presente invención posibilita proporcionar autenticación de red fuerte tal como mecanismos basados en respuesta de desafío sin tener que implicar el AAAh. Además, es opcional si un dominio doméstico y un dominio visitado deciden incorporar una clave compartida temporal como una optimización. Esta decisión de usar una TSK o no, puede basarse en políticas y acuerdos comunes entre el dominio doméstico y el sistema visitado. Un algoritmo común entre un usuario y un dominio visitado es todo lo que se necesita para realizar autenticación y distribución de clave usando una TSK.

Se observa que los ejemplos anteriores se han proporcionado meramente para el fin de explicación y no se han de interpretar de ninguna manera como limitantes de la presente invención. Aunque la presente invención se ha descrito con referencia a una realización preferida, se entiende que las palabras que se han usado en el presente documento son palabras de descripción e ilustración, en lugar de palabras de limitación. Pueden realizarse cambios dentro del ámbito de las reivindicaciones adjuntas, como se establecen actualmente y como modificadas, sin alejarse del alcance de la presente invención en sus aspectos. Aunque la presente invención se ha descrito en el presente documento con referencia a métodos, materiales y realizaciones particulares, la presente invención no se pretende que esté limitada a los detalles particulares desvelados en el presente documento, en su lugar, la presente invención se extiende a todas las estructuras funcionalmente equivalentes, métodos y usos, tales como dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Método, que comprende

- generar una primera clave para un nodo móvil en una red de dominio doméstico de dicho nodo móvil;
- almacenar dicha primera clave en dicha red de dominio doméstico;
- enviar dicha primera clave a dicho nodo móvil por dicha red de dominio doméstico;
- recibir una solicitud para autenticar el nodo móvil desde una red de dominio visitado en dicha red de dominio doméstico;

estando el método adicionalmente **caracterizado por**:

- generar una segunda clave en dicha red de dominio doméstico usando dicha primera clave y un número aleatorio; y
- enviar dicho número aleatorio y dicha segunda clave a dicha red de dominio visitado por dicha red de dominio doméstico.

2. Método, que comprende
al visitar un nodo móvil una red

- enviar una solicitud para autenticar dicho nodo móvil desde dicha red de dominio visitado a una red de dominio doméstico de dicho nodo móvil;

estando el método adicionalmente **caracterizado por**:

- recibir un número aleatorio y una segunda clave desde dicha red de dominio doméstico en dicha red de dominio visitado;
- enviar dicho número aleatorio a dicho nodo móvil por dicha red de dominio visitado; y
- usar dicha segunda clave para al menos un procedimiento de autenticación entre dicho nodo móvil y dicha red de dominio visitado.

3. Método, que comprende

- recibir una primera clave en un nodo móvil desde una red de dominio doméstico de dicho nodo móvil;
- almacenar dicha primera clave en dicho nodo móvil;
- visitar una red por dicho nodo móvil;
- recibir un número aleatorio desde dicha red de dominio visitado en dicho nodo móvil;

estando el método adicionalmente **caracterizado por**:

- generar una segunda clave en dicho nodo móvil usando dicho número aleatorio y dicha primera clave; y
- usar dicha segunda clave para al menos un procedimiento de autenticación entre dicho nodo móvil y dicha red de dominio visitado.

4. Método, que comprende
delegar procedimientos de seguridad a una red de dominio visitado

- generando una primera clave para un nodo móvil;
- almacenando la primera clave en el nodo móvil y en una red de dominio doméstico del nodo móvil;
- moviendo el nodo móvil a la red de dominio visitado;
- enviando una solicitud para autenticar el nodo móvil desde la red de dominio visitado a la red de dominio doméstico;

estando el método adicionalmente **caracterizado por**:

- generar una segunda clave en la red de dominio doméstico usando la primera clave y un número aleatorio y enviar el número aleatorio y la segunda clave a la red de dominio visitado;
- enviar el número aleatorio al nodo móvil por la red de dominio visitado;
- generar la segunda clave por el nodo móvil usando el número aleatorio y la primera clave; y
- usar la segunda clave para al menos un procedimiento de autenticación entre el nodo móvil y la red de dominio visitado.

5. Método de acuerdo con una cualquiera de las reivindicaciones 2 a 4, en el que el procedimiento de autenticación es un procedimiento de derivación de clave.

6. Método de acuerdo con la reivindicación 5, en el que el procedimiento de derivación de clave comprende generar al menos una clave de sesión usando la segunda clave.

7. Método de acuerdo con una cualquiera de las reivindicaciones 2 a 4, en el que el procedimiento de autenticación comprende uno de

- autenticación del nodo móvil por la red de dominio visitado;
- autenticación de la red de dominio visitado por el nodo móvil;
- control de distribución de clave entre el nodo móvil y entidades en la red de dominio visitado por la red de dominio visitado;
- cifrado y protección de integridad de mensajes entre el nodo móvil y una entidad en la red de dominio visitado; y
- distribución de claves dinámicas entre el nodo móvil y entidades en la red de dominio visitado basándose en una asociación de seguridad local.

8. Método de acuerdo con las reivindicaciones 1 o 4, que comprende adicionalmente generar la segunda clave en la red de dominio doméstico usando la primera clave y el número aleatorio como entradas a un algoritmo.

9. Método de acuerdo con una cualquiera de las reivindicaciones 1, 2, 4 y 5 a 8 cuando dependen de las reivindicaciones 1, 2 o 4, en el que el número aleatorio y la segunda clave se envían desde la red de dominio doméstico a la red de dominio visitado a través de un canal seguro.

10. Método de acuerdo con las reivindicaciones 1, 2 o 4, en el que la red de dominio doméstico comprende un servidor de Autenticación, Autorización y Contabilidad, AAA.

11. Método de acuerdo con las reivindicaciones 1, 2 o 4, en el que la red de dominio visitado incluye un servidor de Autenticación, Autorización y Contabilidad, AAA.

12. Método de acuerdo con la reivindicación 11, que comprende adicionalmente comunicar con el nodo móvil por el servidor de AAA a través de un cliente de AAA.

13. Método de acuerdo con la reivindicación 12, en el que el cliente de AAA comprende uno de un asistente localizado en un encaminador, un Agente de Registro y un servidor localizado en la red de dominio visitado.

14. Método de acuerdo con la reivindicación 12, en el que el número aleatorio y la segunda clave se envían a uno de un servidor de AAA y un cliente de AAA.

15. Método de acuerdo con una cualquiera de las reivindicaciones 1 a 4, en el que la segunda clave es una clave compartida temporal, TSK.

16. Método de acuerdo con la reivindicación 4, que comprende adicionalmente:

generar un segundo número aleatorio en la red de dominio doméstico;
generar una tercera clave en la red de dominio doméstico usando la primera clave y el segundo número aleatorio y enviar el segundo número aleatorio y la tercera clave a la red de dominio visitado; y
enviar el segundo número aleatorio al nodo móvil por la red de dominio visitado.

17. Método de acuerdo con la reivindicación 16, en el que generar la tercera clave se basa en las políticas de red de dominio doméstico.

18. Método de acuerdo con la reivindicación 16, que comprende adicionalmente actualizar la segunda clave con la tercera clave en el nodo móvil.

19. Método de acuerdo con la reivindicación 16, que comprende adicionalmente:

- generar una solicitud de autenticación de red por el nodo móvil y enviar la solicitud de autenticación de red a la red de dominio visitado;
- generar una primera respuesta de autenticación por la red de dominio visitado usando la tercera clave y la solicitud de autenticación de red y enviar la respuesta de autenticación de red al nodo móvil;
- generar la tercera clave por el nodo móvil usando la primera clave y el segundo número aleatorio;
- generar una segunda respuesta de autenticación por el nodo móvil usando la tercera clave y la solicitud de autenticación de red;
- comparar la primera respuesta de autenticación generada por la red de dominio visitado con la segunda respuesta de autenticación generada por el nodo móvil, autenticar la red de dominio visitado por el nodo móvil si coinciden la segunda respuesta de autenticación y la primera respuesta de autenticación e indicar a la red de dominio visitado que la segunda clave se ha actualizado con la tercera clave si coinciden la primera respuesta de autenticación y la segunda respuesta de autenticación; y
- usar la tercera clave por la red de dominio visitado para los procedimientos de autenticación entre el nodo móvil y la red de dominio visitado.

20. Método de acuerdo con la reivindicación 19, que comprende adicionalmente enviar un informe a la red de dominio visitado de que la segunda clave se ha actualizado.

21. Método de acuerdo con la reivindicación 16, en el que la tercera clave es una clave compartida temporal, TSK.

22. Método de acuerdo con la reivindicación 18, que comprende adicionalmente:

- generar un tercer número aleatorio por la red de dominio visitado y enviar el tercer número aleatorio al nodo móvil;
- generar segundos datos de autenticación por el nodo móvil usando el tercer número aleatorio y la tercera clave y enviar los segundos datos de autenticación a la red de dominio visitado; y
- usar los segundos datos de autenticación por la red de dominio visitado para verificar que el nodo móvil ha actualizado la segunda clave con la tercera clave.

23. Método de acuerdo con la reivindicación 22, que comprende adicionalmente enviar un informe a la red de dominio doméstico de que la segunda clave se ha sustituido por la tercera clave.

24. Método de acuerdo con la reivindicación 4, que comprende adicionalmente:

- usar la segunda clave para generar primeros datos de autenticación por el nodo móvil;
- generar un desafío de anfitrión para autenticar la red de dominio doméstico y enviar los primeros datos de autenticación, el desafío de anfitrión y una identidad de nodo móvil desde el nodo móvil a la red de dominio visitado;
- enviar los primeros datos de autenticación, el desafío de anfitrión y la identidad de nodo móvil desde la red de dominio visitado a la red de dominio doméstico;
- generar segundos datos de autenticación y usar el desafío de anfitrión y la primera clave, en la red de dominio doméstico;
- enviar los segundos datos de autenticación desde la red de dominio doméstico a la red de dominio visitado, reenviando la red de dominio visitado los segundos datos de autenticación al nodo móvil; y
- usar los segundos datos de autenticación para verificar la red de dominio doméstico por el nodo móvil.

25. Elemento de red en una red de dominio doméstico de un nodo móvil, que comprende

- medios para generar una primera clave para dicho nodo móvil;
- medios para almacenar dicha primera clave;
- medios para enviar dicha primera clave a dicho nodo móvil;
- medios para recibir una solicitud para autenticar el nodo móvil desde una red de dominio visitado visitada por dicho nodo móvil;

adicionalmente **caracterizado por**:

- medios para generar una segunda clave en dicha red de dominio doméstico usando dicha primera clave y un número aleatorio; y
- medios para enviar dicho número aleatorio y dicha segunda clave a dicha red de dominio visitado.

26. Elemento de red en una red de dominio visitado visitada por un nodo móvil, que comprende

- medios para, al visitar dicho nodo móvil dicha red de dominio visitado, enviar una solicitud para autenticar dicho nodo móvil a una red de dominio doméstico de dicho nodo móvil;

adicionalmente **caracterizado por**:

- medios para recibir un número aleatorio y una segunda clave desde dicha red de dominio doméstico;
- medios para enviar dicho número aleatorio a dicho nodo móvil; y
- medios para usar dicha segunda clave para al menos un procedimiento de autenticación entre dicho nodo móvil y dicha red de dominio visitado.

27. Nodo móvil, que comprende

- medios para recibir una primera clave desde una red de dominio doméstico de dicho nodo móvil;
- medios para almacenar dicha primera clave;
- medios para, al visitar una red de dominio visitado, recibir un número aleatorio desde dicha red de dominio visitado;

adicionalmente **caracterizado por**:

- medios para generar una segunda clave usando dicho número aleatorio y dicha primera clave; y
- medios para usar dicha segunda clave para al menos un procedimiento de autenticación entre dicho nodo móvil y dicha red de dominio visitado.

28. Sistema, que comprende:

- una red de dominio doméstico, conteniendo la red de dominio doméstico al menos un servidor;
- un nodo móvil, compartiendo el nodo móvil una primera clave con dicho al menos un servidor en la red de dominio doméstico; y
- una red de dominio visitado, conteniendo la red de dominio visitado al menos un segundo servidor, existiendo una asociación de seguridad entre dicho al menos un servidor en la red de dominio doméstico y dicho al menos un segundo servidor en la red de dominio visitado;

en el que la red de dominio visitado está adaptada, cuando el nodo móvil hace itinerancia en la red de dominio visitado, para solicitar autenticación del nodo móvil por la red de dominio doméstico, adicionalmente **caracterizado por**: estar adaptado dicho al menos un servidor en la red de dominio doméstico para generar una segunda clave usando la primera clave y enviar la segunda clave a la red de dominio visitado, estando adaptados dicho nodo móvil y dicho segundo servidor para usar la segunda clave para al menos un procedimiento de autenticación entre el nodo móvil y la red de dominio visitado.

29. Sistema de acuerdo con una cualquiera de las reivindicaciones 26 a 28, en el que el procedimiento de autenticación es un procedimiento de derivación de clave.

30. Sistema de acuerdo con la reivindicación 29, en el que el procedimiento de derivación de clave comprende generar al menos una clave de sesión usando la segunda clave.

31. Sistema de acuerdo con la reivindicación 28 o elemento de red de acuerdo con la reivindicación 25, en donde dicho al menos un servidor en la red de dominio doméstico comprende un servidor de Autenticación, Autorización y Contabilidad, AAA.

32. Sistema de acuerdo con la reivindicación 28 o elemento de red de acuerdo con la reivindicación 26, en donde dicho al menos un segundo servidor en la red de dominio visitado comprende un servidor de Autenticación Autorización y Contabilidad, AAA.

33. Sistema de acuerdo con la reivindicación 28 o nodo móvil de acuerdo con la reivindicación 27, en donde el nodo móvil comprende un teléfono móvil.

34. Sistema, elemento de red o nodo móvil de acuerdo con una cualquiera de las reivindicaciones 25 a 28, en donde la segunda clave es una clave compartida temporal, TSK.

35. Sistema de acuerdo con la reivindicación 28 o elemento de red de acuerdo con las reivindicaciones 25 o 26, en donde el procedimiento de autenticación comprende

- autenticación del dispositivo móvil por la red de dominio visitado;
- autenticación de la red de dominio visitado por el dispositivo móvil;
- control por la red de dominio visitado de la distribución de clave entre el dispositivo móvil y entidades en la red de dominio visitado;
- cifrado y protección de integridad de mensajes entre el dispositivo móvil y una entidad en la red de dominio visitado;
- distribución de claves dinámicas entre el dispositivo móvil y entidades en la red de dominio visitado basándose en una asociación de seguridad local.

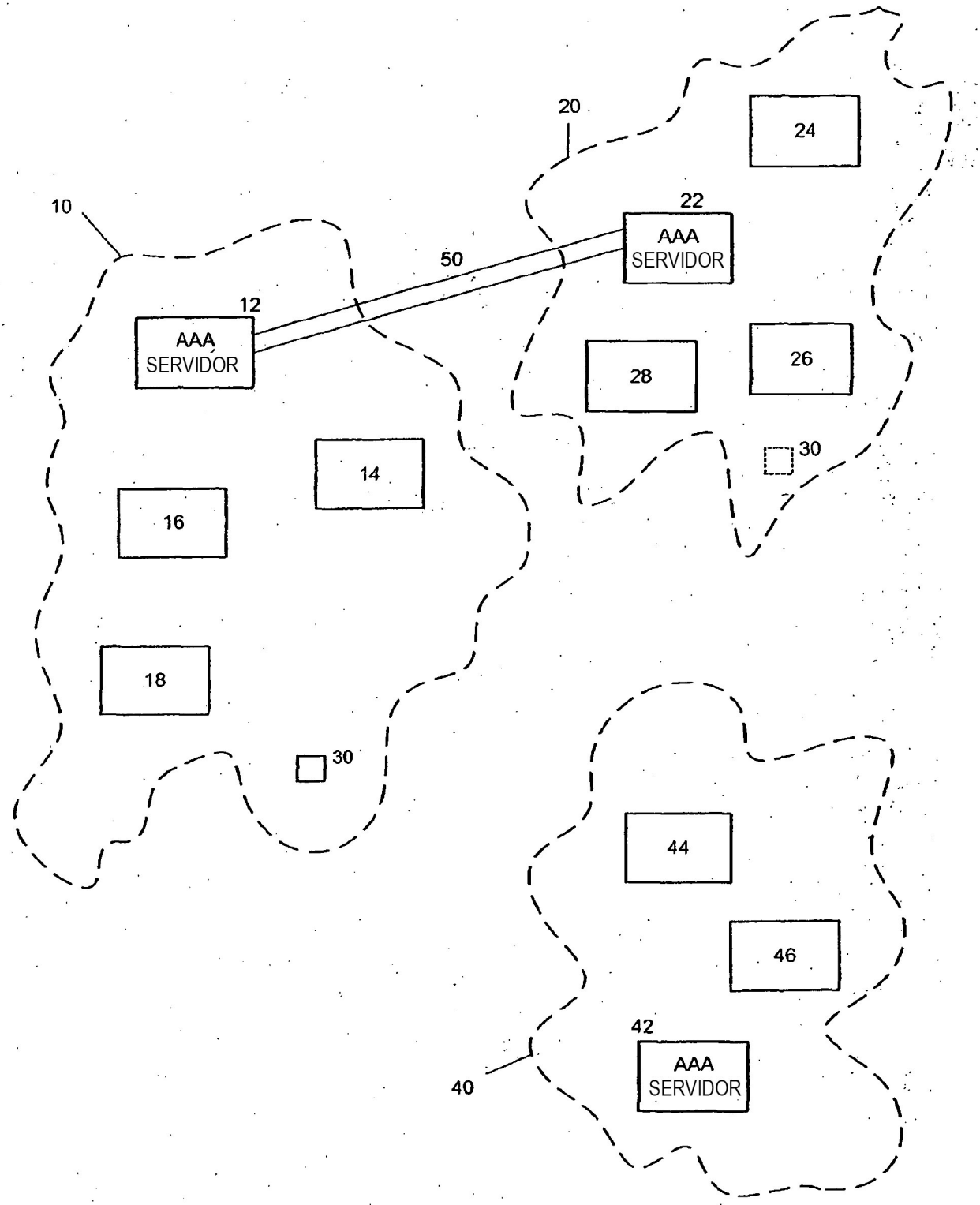

10
20
24
22
AAA
SERVIDOR
50
12
AAA
SERVIDOR
28
26
30
14
16
18
30
44
46
42
AAA
SERVIDOR
40

FIG. 1

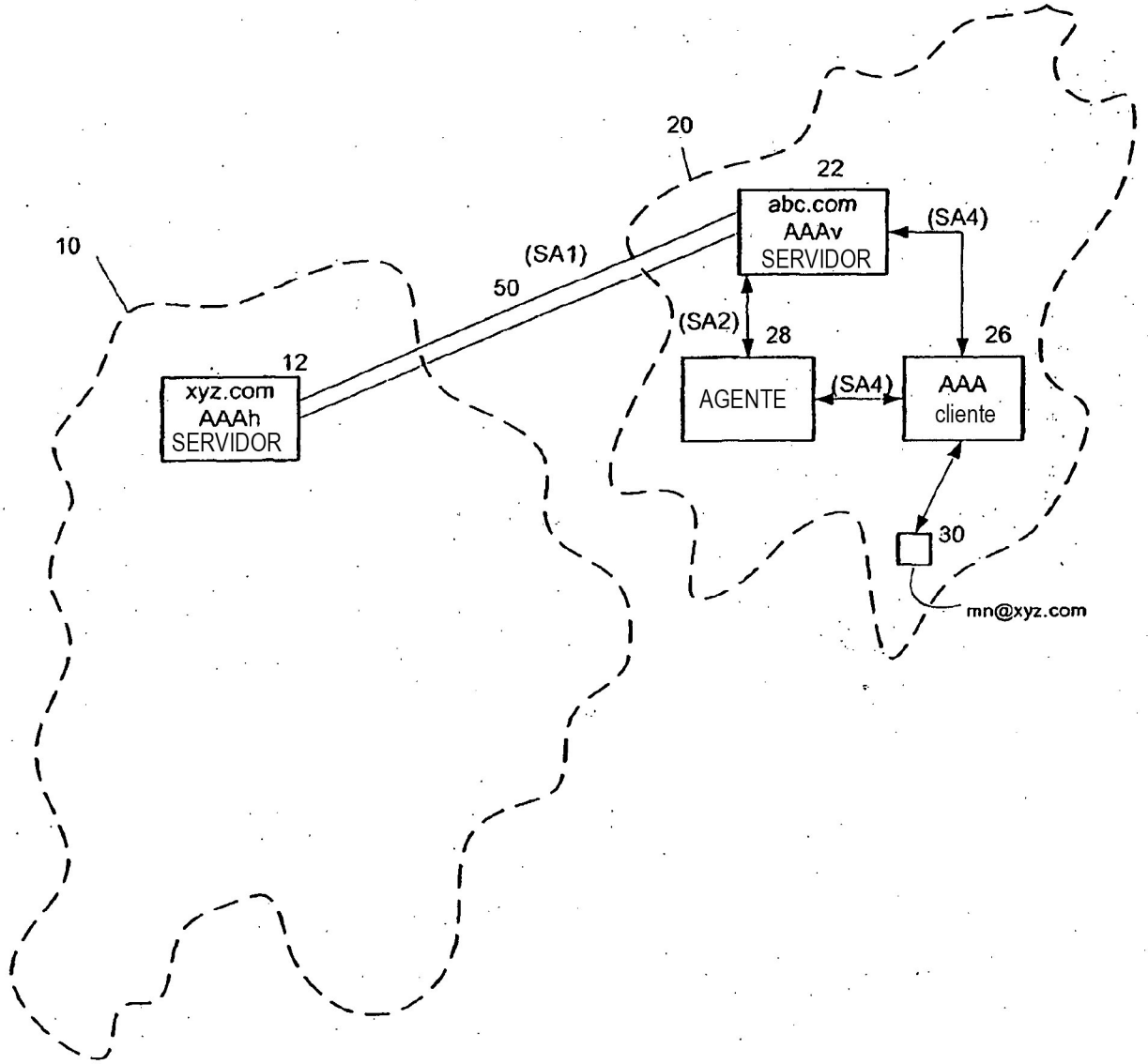

10
20
22
abc.com
AAAv
SERVIDOR
(SA4)
(SA1)
50
(SA2)
28
26
12
xyz.com
AAAh
SERVIDOR
AGENTE
(SA4)
AAA
cliente
30
mn@xyz.com

FIG. 2

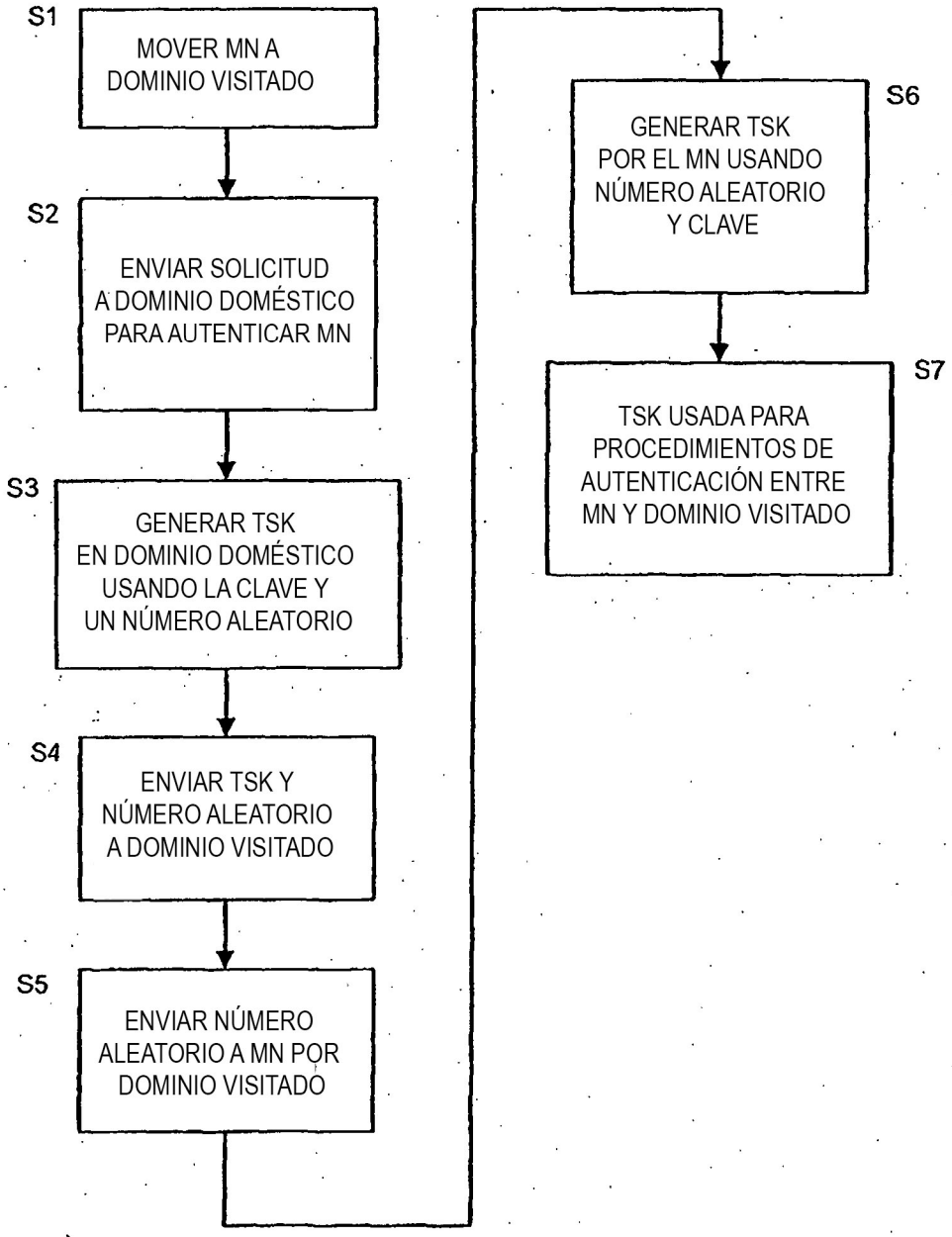
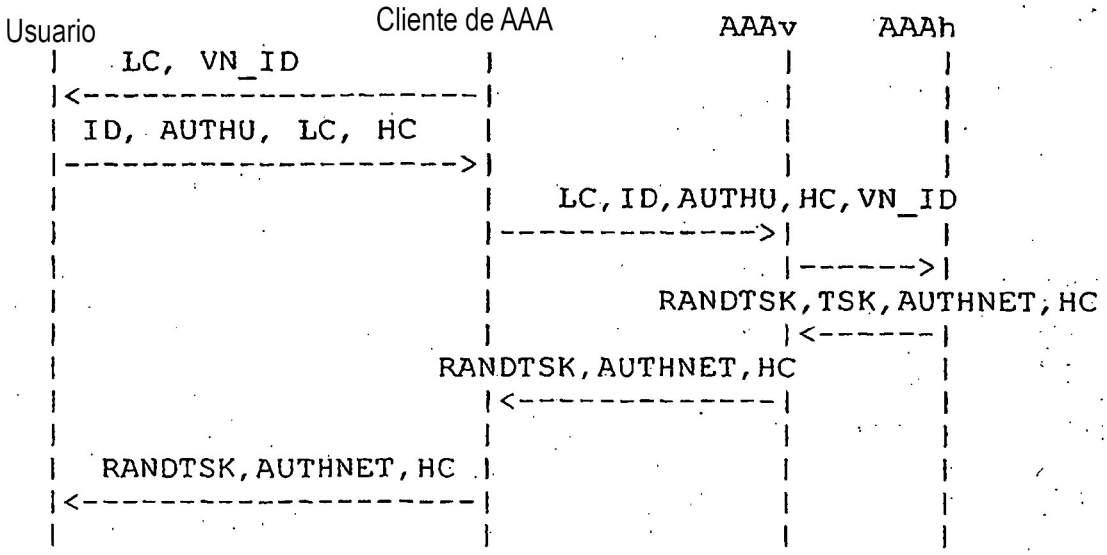

S1
MOVER MN A DOMINIO VISITADO
S2
ENVIAR SOLICITUD A DOMINIO DOMÉSTICO PARA AUTENTICAR MN
S3
GENERAR TSK EN DOMINIO DOMÉSTICO USANDO LA CLAVE Y UN NÚMERO ALEATORIO
S4
ENVIAR TSK Y NÚMERO ALEATORIO A DOMINIO VISITADO
S5
ENVIAR NÚMERO ALEATORIO A MN POR DOMINIO VISITADO
S6
GENERAR TSK POR EL MN USANDO NÚMERO ALEATORIO Y CLAVE
S7
TSK USADA PARA PROCEDIMIENTOS DE AUTENTICACIÓN ENTRE MN Y DOMINIO VISITADO

FIG. 3



LC = Desafío local
HC = Desafío de anfitrión
AUTHU = Datos de autenticación de usuario
ID = Identificador de usuario
VN_ID = Identificador de red visitada
AUTHNET = Datos de autenticación de red

FIG. 4

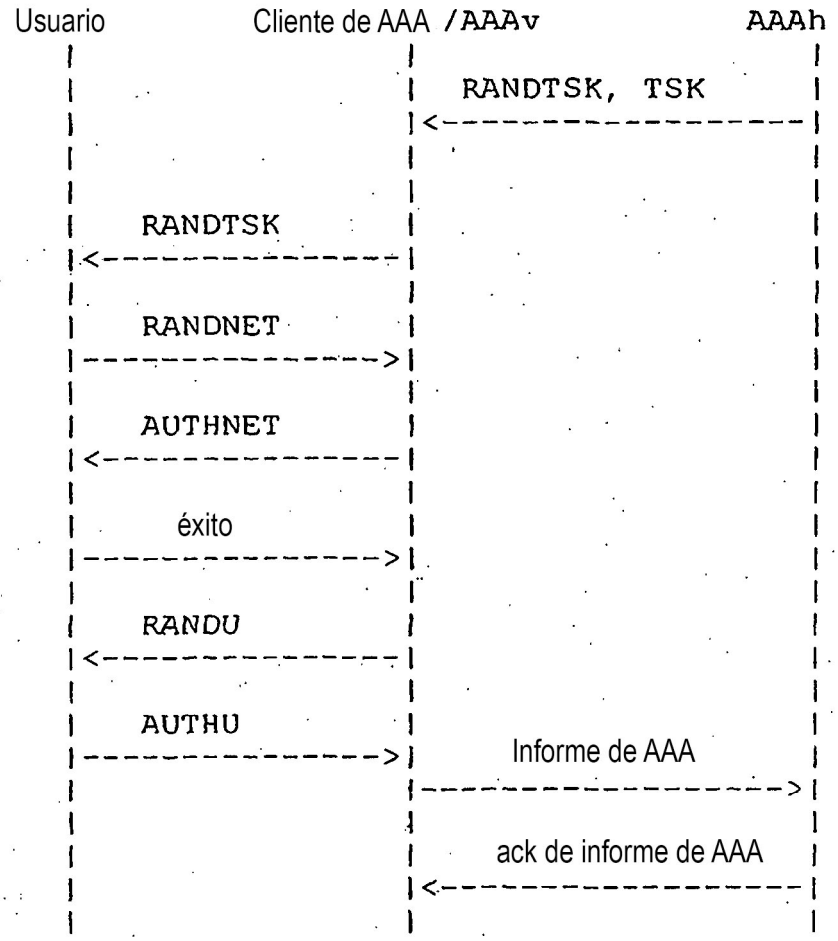

Usuario
Cliente de AAA /AAAv
AAAh
RANDTSK, TSK
RANDTSK
RANDNET
AUTHNET
éxito
RANDU
AUTHU
Informe de AAA
ack de informe de AAA

FIG. 5