(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 397 063**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.03.2003 E 03747179 (4)**

(97) Fecha y número de publicación de la concesión europea: **07.11.2012 EP 1514194**

(54) Título: **Autenticación para protocolos de aplicación IP basados en procedimientos IMS del 3GPP**

(30) Prioridad:

26.04.2002 US 132226

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.03.2013

(73) Titular/es:

NOKIA CORPORATION (100.0%)
Keilalahdentie 4
02150 Espoo, FI

(72) Inventor/es:

ISOMAKI, MARKUS;
COSTA-REQUENA, JOSE;
LANSISALMI, ATTE;
NIEMI, VALTTERI;
NIEMI, AKI;
HAUKKA, TAO;
BAJKO, GABOR y
VIITANEN, TOMMI

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Autenticación para protocolos de aplicación IP basados en procedimientos IMS del 3GPP.

La presente invención se refiere a la autenticación de las solicitudes de servicios de datos desde al menos un equipo de usuario que usa múltiples protocolos.

Antecedentes de la técnica

La memoria descriptiva técnica del 3GPP TS 33.203 v1.0.0 (12-2001), que se incorpora en el presente documento como referencia en su totalidad, autentica los clientes del subsistema de red de núcleo multimedia IP (IMS) ejecutando el protocolo de acuerdo de autenticación y claves (AKA) durante una transacción de registro SIP. Véase la sección 6.1 para una discusión del AKA. Después de que la autenticación usando AKA se ha completado, la clave de integridad (IK) y la clave de cifrado (CK) creadas se comparten entre el equipo de usuario (UE) y la función de control del estado de la llamada de intermediario (PCSCF), que es la primera entidad en una red SIP que recibe una solicitud de una sesión desde el UE. El P-CSCF puede estar de manera residente en o una red residencial o en una red visitada. Las solicitudes SIP de servicios se protegen mediante las claves IK y CK hasta que las claves se renuevan mediante otra transacción de registro. Las claves IK y CK se distribuyen de una forma segura mediante cualquier técnica bien conocida, tal como IP Sec o EPS.

Las principales entidades SIP usadas para el registro del UE son: el UE, la P-CSCF, la función de control del estado de la llamada de servicio (S-CSCF) y un servidor de abonado residencial (HSS). El UE comunica con la P-CSCF, que se comunica con la S-CSCF que se comunica con el HSS. Una descripción detallada de la autenticación y del registro se encuentra en las secciones 4 y 5-5.2 de la especificación citada.

Con la llegada de los servicios multimedia IP (IM), es deseable que los UE que usan SIP tengan acceso a los servicios de datos usando protocolos adicionales, tales como el protocolo de transferencia de hipertexto (HTTP) y el protocolo de flujo en tiempo real (RTSP). Una descripción del RTSP se encuentra en la RFC 2326 fechada en 1998, que se incorpora en el presente documento como referencia en su totalidad.

Básico para el acceso del UE a los servicios de red que implican cualquier protocolo, tal como SIP, HTTP y RTSP, es la necesidad de autenticación del UE y la seguridad. El estado de la técnica en la actualidad es que cada protocolo utiliza su propia seguridad y medidas de autenticación, cuando se hace una solicitud mediante el UE de una sesión de servicios de datos. Cuando un UE es un solicitante de servicios de datos que implica múltiples protocolos, se necesitan entidades de red específicas del protocolo individual en forma de un servidor intermediario o, de otro modo, realizar la autenticación para cada protocolo. Las múltiples entidades requeridas actualmente para la autenticación de la UE para obtener sesiones que implican múltiples protocolos, pueden tener diferentes direcciones de red, implican una duplicación de procesamiento por cada intermediario para obtener la información de autenticación.

El documento de Estados Unidos 6.308.203 B1 *enseña a proporcionar información personal de un usuario a un proveedor de información desde cualquier localización, así como, para hacer innecesario a un dispositivo terminal del usuario introducir la información personal. De ese modo, se usa un dispositivo de intermediario que presenta una capacidad de servicio de agente de intermediario para proporcionar la información personal junto con una base de datos de perfiles de usuario.*

El documento EP 0 924 630 A1 *se refiere a la recuperación de recursos a través de una red de datos mediante descargando los recursos a un cliente desde un servidor de contenidos a través de la red de datos. De ese modo, el derecho del cliente a recibir el recurso solicitado se autentica en términos de restricciones de facturación y/o de acceso en un intermediario.*

Sumario de la invención

De acuerdo con diversos aspectos de la presente invención, se proporciona un sistema, un procedimiento y un servidor intermediario, tal como se define en las reivindicaciones adjuntas.

La presente invención *se refiere a* un sistema, un procedimiento, y al menos un servidor intermediario que proporciona autenticación a las sesiones del UE de los servicios de datos que requieren múltiples protocolos que usan la información de autenticación común para cada uno de los múltiples protocolos. Se usa al menos un servidor intermediario para autenticar las solicitudes de sesiones de servicios de datos del UE para los múltiples protocolos. Mientras que la arquitectura más simple que puede usarse para practicar la invención es un único servidor intermediario, debería entenderse que puede usarse más de un servidor intermediario para realizar la autenticación de los servicios de datos del UE para los múltiples protocolos usando la información de autenticación común.

Al menos un servidor intermediario almacena información de autenticación desde un servidor de datos de abonado de una red residencial para al menos un UE requerido de un primer protocolo.

Al menos un servidor intermediario autentica las solicitudes de las sesiones de servicios de datos recibidas desde al

menos un UE para los protocolos que no sea el primer protocolo usando la información de autenticación obtenida del servidor de datos de abonado para el primer protocolo. Las sesiones de autenticación implican transacciones IMS que se realizan fácilmente mediante al menos un servidor intermediario para los protocolos que no sea el primer protocolo.

Al menos un servidor intermediario proporciona acceso a los usuarios de los servicios IMS con un protocolo (por ejemplo, HTTP) diferente de SIP (como se usa, normalmente, en IMS). Los servicios IMS incluyen diferentes estructuras de datos (XML, SOAP, ACAP, etc.) para realizar tareas de gestión de servicios como la manipulación de políticas de autorización, gestión de la lista de miembros, etc. Esto es necesario para la gestión de datos que requieren un protocolo fiable como HTTP, sin dejar de aplicar los mecanismos de seguridad específicos de IMS. Al menos un servidor intermediario autentica el mensaje de acuerdo con las especificaciones y algoritmos de IMS y pasa el contenido al servidor de aplicaciones correcto usando otro protocolo diferente de SIP, como HTTP (por ejemplo, aplicaciones de presencia, mensajería o un servidor de conferencia) que implementa el propio servicio.

Al menos un servidor intermediario también añade información, preferentemente, en forma de un par de claves secretas compartidas u otro mecanismo de seguridad, que al menos un servidor de aplicaciones, por ejemplo, un servidor HTTP o RTSP, puede usar para asegurar la identidad del usuario que se autentica y emitió la solicitud de los servicios usando el protocolo particular. Al menos un servidor de aplicaciones tiene la responsabilidad final de autorizar al usuario y/o a la acción a realizar por el servidor de aplicaciones para el usuario.

En una realización preferida, el primer protocolo es SIP y al menos un protocolo adicional es uno o ambos de HTTP y RTSP. Las solicitudes de sesiones de servicios de datos que usan SIP se transmiten desde la P-CSCF, residente en al menos un servidor intermediario, a un servidor S-CSCF de la red residencial y a continuación al HSS. Las solicitudes de sesiones de servicios de datos que usan el protocolo HTTP usan la información de autenticación SIP y se transmiten desde un intermediario del protocolo de transferencia de hipertexto (HTTP) de al menos un servidor intermediario a un servidor HTTP. Las solicitudes de sesiones de servicios de datos que usan el protocolo RTSP usan la información de autenticación SIP y se transmiten desde un intermediario del protocolo de transmisión en tiempo real (RTSP) del servidor intermediario a un servidor RTSP.

La información de autenticación preferida transmitida desde el HSS a, al menos, un servidor intermediario comprende, una clave de integridad (IK) y una clave de cifrado (CK). La transmisión de información de autenticación desde al menos un UE a, al menos, un servidor intermediario comprende también, la clave de integridad (IK) y la clave de cifrado (CK). Las claves se procesan mediante al menos un servidor intermediario para determinar si al menos un UE es auténtico.

La invención elimina la necesidad de información de autenticación única de cada protocolo para autenticar las sesiones de datos del UE. En una realización preferida un único servidor intermediario incluye todos los intermediarios de los protocolos residentes, en el mismo. La información de autenticación para los protocolos adicionales, por ejemplo, HTTP y RTSP, se obtiene a partir de la información de autenticación SIP de al menos un UE.

La invención es un sistema que incluye una red residencial que incluye un servidor de datos de abonado que almacena al menos un perfil de usuario en lo concerniente a proporcionar servicios de datos a, al menos, un usuario con el perfil que incluye la información de autenticación usada para autenticar a, al menos, un usuario de los servicios de datos cuando se hace una solicitud de los servicios de datos usando un primer protocolo; al menos un equipo de usuario solicita los servicios de datos usando el primer protocolo y los servicios de datos usando al menos un protocolo adicional, al menos un equipo de usuario que almacena la información de autenticación que se usa cuando se hace una solicitud de los servicios de datos para autenticar a, al menos, un usuario; al menos un servidor intermediario que incluye de manera residente, en el mismo, un primer intermediario del primer protocolo de red y al menos un intermediario adicional de al menos un protocolo adicional; y en el que el primer intermediario y al menos un intermediario adicional del servidor intermediario autentica las solicitudes de los servicios de datos recibidos desde al menos un equipo de usuario de los protocolos usando la información de autenticación de al menos un perfil que se transmite desde el servidor de datos de abonado a, al menos, un servidor intermediario y la información de autenticación de al menos un usuario transmitida desde al menos un equipo de usuario a, al menos, un servidor intermediario. El servidor de datos de abonado puede ser un servidor de abonado residencial (HSS); y el primer protocolo puede ser el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP puede transmitirse desde una función de control del estado de la llamada de intermediario (P-CSCF) de al menos un servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial. El servidor de datos de abonado puede ser un servidor de abonado residencial (HSS); el primer protocolo puede ser el protocolo de inicio de sesión (SIP) y una solicitud de datos de los servicios de datos que usa SIP se transmite desde una función de control del estado de la llamada de intermediario (P-CSCF) de al menos un servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial; y al menos un protocolo adicional puede ser el protocolo de transferencia de hipertexto (HTTP) y una solicitud de servicios de datos que usa HTTP puede transmitirse desde un intermediario del protocolo de transferencia de hipertexto (HTTP) de al menos un servidor intermediario a un servidor HTTP. El servidor de datos de abonado puede ser un servidor de abonado residencial (HSS); el primer protocolo puede ser el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP puede transmitirse desde una función de control

del estado de la llamada de intermediario (P-CSCF) de al menos un servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF); y al menos un protocolo adicional que puede ser el protocolo de transmisión en tiempo real (RTSP) y una solicitud de servicios de datos que puede transmitirse desde un intermediario del protocolo de transmisión en tiempo real (RTSP) de al menos un servidor intermediario a un servidor RTSP. El servidor de datos de abonado puede ser un servidor de abonado residencial (HSS); el primer protocolo puede ser el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP puede transmitirse desde una función de control del estado de la llamada de intermediario (P-CSCF) de al menos un servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial; y al menos un protocolo adicional puede ser el protocolo de transferencia de hipertexto (HTTP) y el protocolo de transmisión en tiempo real (RTSP) y una solicitud de servicios de datos que usa HTTP puede transmitirse desde un intermediario del protocolo de transferencia de hipertexto (HTTP) de al menos un servidor intermediario a un servidor HTTP y una solicitud de servicios de datos que usa RTSP puede transmitirse desde el intermediario del protocolo de transmisión en tiempo real (RTSP) de al menos un servidor intermediario a un servidor RTSP. La información de autenticación transmitida desde el servidor de datos de abonado a, al menos, un servidor intermediario puede comprender una clave de integridad IK y una clave de cifrado CK y la información de autenticación transmitida desde al menos un equipo de usuario a, al menos, un servidor intermediario puede comprender una clave de integridad IK y una clave de cifrado CK cuyas claves se procesan mediante al menos un servidor intermediario para determinar si al menos un usuario es auténtico. La información de autenticación transmitida desde el servidor de datos de abonado y al menos un equipo de usuario puede generarse usando el protocolo de acuerdo de autenticación y claves (AKA).

En un sistema que comprende una red residencial que incluye un servidor de datos de abonado que almacena, al menos, un perfil de usuario en lo concerniente a proporcionar servicios de datos a, al menos, un usuario con el perfil que incluye la información de autenticación usada para autenticar a, al menos, un usuario de los servicios de datos cuando se hace una solicitud de los servicios de datos usando un primer protocolo y al menos un equipo de usuario que solicita los servicios de datos usando el primer protocolo de red y los servicios de datos usando al menos un protocolo adicional, al menos un equipo de usuario que almacena la información de autenticación que se usa cuando se hace una solicitud de servicios de datos para autenticar a, al menos, un usuario; al menos un servidor intermediario que incluye de manera residente, en el mismo, un primer intermediario del primer protocolo de red y al menos un intermediario adicional de, al menos, un protocolo adicional, un procedimiento de autenticación de al menos un equipo de usuario incluye el primer intermediario y al menos un intermediario adicional de al menos un servidor intermediario que autentica las solicitudes de los servicios de datos recibidos desde al menos un equipo de usuario de los protocolos usando la información de autenticación de al menos un perfil que se transmite desde el servidor de datos de abonado a, al menos, un servidor intermediario y la información de autenticación de al menos un usuario transmitida desde al menos un equipo de usuario a, al menos, un servidor intermediario. El servidor de datos de abonado puede ser un servidor de abonado residencial (HSS); el primer protocolo puede ser el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP puede transmitirse desde una función de control del estado de la llamada de intermediario (P-CSCF) de al menos un servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial; y al menos un protocolo de red adicional puede ser el protocolo de transferencia de hipertexto (HTTP) y una solicitud de servicios de datos que usa HTTP puede transmitirse desde un intermediario del protocolo de transferencia de hipertexto (HTTP) de al menos un servidor intermediario a un servidor HTTP. El servidor de datos de abonado puede ser un servidor de abonado residencial (HSS); el primer protocolo puede ser el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP puede transmitirse desde una función de control del estado de la llamada de intermediario (P-CSCF) de al menos un servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF); y al menos un protocolo adicional que puede ser el protocolo de transmisión en tiempo real (RTSP) y una solicitud de servicios de datos que puede transmitirse desde un intermediario del protocolo de transmisión en tiempo real (RTSP) de al menos un servidor intermediario a un servidor RTSP. El servidor de datos de abonado puede ser un servidor de abonado residencial (HSS); el primer protocolo puede ser el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP puede transmitirse desde una función de control del estado de la llamada de intermediario (P-CSCF) de al menos un servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial; y al menos un protocolo adicional puede ser el protocolo de transferencia de hipertexto (HTTP) y el protocolo de transmisión en tiempo real (RTSP) y una solicitud de servicios de datos que usa HTTP puede transmitirse desde un intermediario del protocolo de transferencia de hipertexto (HTTP) de al menos un servidor intermediario a un servidor HTTP y una solicitud de servicios de datos que usa RTSP puede transmitirse desde el intermediario del protocolo de transmisión en tiempo real (RTSP) de al menos un servidor intermediario a un servidor RTSP. La información de autenticación transmitida desde el servidor de datos de abonado a, al menos, un servidor intermediario puede comprender una clave de integridad IK y una clave de cifrado CK y la información de autenticación transmitida desde al menos un equipo de usuario a, al menos, un servidor intermediario puede comprender una clave de integridad IK y una clave de cifrado CK cuyas claves se procesan mediante al menos un servidor intermediario para determinar si al menos un usuario es auténtico. La información de autenticación transmitida desde el servidor de datos de abonado y al menos un equipo de usuario puede generarse usando el protocolo de acuerdo de autenticación y claves (AKA).

En un sistema que comprende una red residencial que incluye un servidor de datos de abonado que almacena, al menos, un perfil de usuario en lo concerniente a proporcionar servicios de datos a, al menos, un usuario con el perfil

que incluye la información de autenticación usada para autenticar a, al menos, un usuario de los servicios de datos cuando se hace una solicitud de los servicios de datos usando un primer protocolo y al menos un equipo de usuario que solicita los servicios de datos usando el primer protocolo de red y los servicios de datos usando al menos un protocolo adicional, al menos un equipo de usuario que almacena la información de autenticación que se usa cuando se hace una solicitud de servicios de datos para autenticar a, al menos, un usuario, al menos un servidor intermediario de acuerdo con la invención incluye un primer intermediario del primer protocolo de red y al menos un intermediario adicional de, al menos, un protocolo adicional que están residentes en al menos un servidor intermediario; y en el que el primer intermediario y al menos un intermediario adicional del servidor intermediario autentica las solicitudes de los servicios de datos recibidos desde al menos un equipo de usuario de los protocolos usando la información de autenticación de al menos un perfil que se transmite desde el servidor de datos de abonado a, al menos, un servidor intermediario y la información de autenticación de al menos un usuario transmitida desde al menos un equipo de usuario a, al menos, un servidor intermediario. El servidor de datos de abonado puede ser un servidor de abonado residencial (HSS); y el primer protocolo puede ser el protocolo de inicio de sesión (SIP) y cualquier solicitud de servicios de datos que usa SIP puede transmitirse desde una función de control del estado de la llamada de intermediario (P-CSCF) de al menos un servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial. El servidor de datos de abonado puede ser un servidor de abonado residencial (HSS); y el primer protocolo puede ser el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP puede transmitirse desde una función de control del estado de la llamada de intermediario (P-CSCF) de al menos un servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial; y al menos un protocolo de red adicional puede ser el protocolo de transferencia de hipertexto (HTTP) y una solicitud de servicios de datos que usa HTTP puede transmitirse desde un intermediario del protocolo de transferencia de hipertexto (HTTP) de al menos un servidor intermediario a un servidor HTTP. El servidor de datos de abonado puede ser un servidor de abonado residencial (HSS); y el primer protocolo puede ser el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP puede transmitirse desde al menos un servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF), y al menos un protocolo adicional puede ser el protocolo de transmisión en tiempo real (RTSP) y una solicitud de servicios de datos que puede transmitirse desde un intermediario del protocolo de transmisión en tiempo real (RTSP) de al menos un servidor intermediario a un servidor RTSP. El servidor de datos de abonado puede ser un servidor de abonado residencial (HSS); y el primer protocolo puede ser el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP puede transmitirse desde una función de control del estado de la llamada de intermediario (P-CSCF) de al menos un servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial, y al menos un protocolo adicional puede ser el protocolo de transferencia de hipertexto (HTTP) y el protocolo de transmisión en tiempo real (RTSP) y una solicitud de servicios de datos que usa HTTP puede transmitirse desde un intermediario del protocolo de transferencia de hipertexto (HTTP) de al menos un servidor intermediario a un servidor HTTP y una solicitud de servicios de datos que usa RTSP puede transmitirse desde al menos un servidor intermediario a un servidor RTSP. La información de autenticación puede transmitirse desde el servidor de datos de abonado a, al menos, un servidor intermediario que puede comprender una clave de integridad IK y una clave de cifrado CK y la información de autenticación transmitida desde al menos un equipo de usuario a, al menos, un servidor intermediario puede comprender una clave de integridad IK y una clave de cifrado CK cuyas claves se procesan mediante al menos un servidor intermediario para determinar si al menos un usuario es auténtico. La información de autenticación transmitida desde el servidor de datos de abonado y al menos un equipo de usuario puede generarse usando el protocolo de acuerdo de autenticación y claves (AKA).

Un sistema de acuerdo con la invención incluye una red residencial que incluye un servidor de datos de abonado que almacena al menos un perfil de usuario en lo concerniente a proporcionar servicios de datos a, al menos, un usuario con el perfil que incluye la información de autenticación usada para autenticar a, al menos, un usuario de los servicios de datos cuando se hace una solicitud de los servicios de datos usando un primer protocolo; y al menos un equipo de usuario que solicita los servicios de datos usando el primer protocolo de red y los servicios de datos usando al menos un protocolo adicional, al menos un equipo de usuario que almacena la información de autenticación que se usa cuando se hace una solicitud de servicios de datos para autenticar a, al menos, un usuario; al menos un servidor intermediario, que incluye de manera residente, en el mismo, un primer intermediario del primer protocolo de red y al menos un intermediario adicional de, al menos, un protocolo adicional; al menos un servidor de aplicaciones acoplado a, al menos, un servidor intermediario, cada servidor de aplicaciones proporciona servicios de datos a, al menos, un usuario usando al menos uno de los al menos un protocolos adicionales a través de al menos un servidor intermediario; el primer intermediario y al menos un intermediario adicional de al menos un servidor intermediario que autentica las solicitudes de servicios de datos recibidas desde al menos un equipo de usuario de los protocolos usando la información de autenticación de al menos un perfil que se transmite desde el servidor de datos de abonado a, al menos, un servidor intermediario y la información de autenticación de al menos un usuario transmitida desde al menos un equipo de usuario a, al menos, un servidor intermediario y proporciona información a, al menos, un servidor de aplicaciones permitiendo a, al menos, un servidor de aplicaciones proporcionar la autorización final de al menos un usuario para acceder a, al menos, un servidor de aplicaciones o para proporcionar la autorización final de una acción a realizarse por al menos un usuario mediante al menos un servidor de aplicaciones. Al menos un servidor intermediario puede procesar la información de autenticación para proporcionar la información a, al menos, un servidor de aplicaciones para permitir a, al menos, un servidor de aplicaciones proporcionar la autorización final que incluye la garantía de la identidad de al menos un usuario. El procesamiento de

la información de autenticación proporciona la información a, al menos, un servidor de aplicaciones que puede comprender un secreto compartido conocido para, al menos, un servidor intermediario y al menos un servidor de aplicaciones que garantiza la identidad de al menos un usuario en al menos un servidor de aplicaciones. El secreto compartido puede ser un par de claves compartidas que se procesan mediante al menos un servidor de aplicaciones para verificar la identidad del usuario que va a recibir el acceso a, al menos, un servidor de aplicaciones o para quien al menos un servidor de aplicaciones toma la acción. El acoplamiento de al menos un servidor intermediario a, al menos, un servidor de aplicaciones puede ser a través de un medio seguro. Al menos un servidor de aplicaciones puede registrar servicios de datos con al menos un servidor intermediario que al menos un servidor de aplicaciones puede proporcionar a, al menos, un usuario a través de al menos un servidor intermediario; y al menos un servidor intermediario puede almacenar una dirección de cada servidor de aplicaciones que proporciona los servicios de datos para su selección por al menos un usuario que se usa para conectar al menos un usuario a, al menos, un servidor de aplicaciones para obtener los servicios de datos seleccionados. Al menos un servidor intermediario puede ser un punto de acceso en el sistema para la transmisión de los servicios de datos entre al menos un usuario y al menos un servidor intermediario.

En un sistema que comprende una red residencial que incluye un servidor de datos de abonado que almacena al menos un perfil de usuario en lo concerniente a proporcionar servicios de datos a, al menos, un usuario con el perfil que incluye la información de autenticación usada para autenticar a, al menos, un usuario de los servicios de datos cuando se hace una solicitud de los servicios de datos usando un primer protocolo y al menos un equipo de usuario que solicita los servicios de datos usando el primer protocolo de red y los servicios de datos usando al menos un protocolo adicional, al menos un equipo de usuario que almacena la información de autenticación que se usa cuando se hace una solicitud de servicios de datos para autenticar a, al menos, un usuario, al menos un servidor intermediario que incluye de manera residente, en el mismo, un primer intermediario del primer protocolo de red y al menos un intermediario adicional de, al menos, un protocolo adicional, y al menos un servidor de aplicaciones acoplado a, al menos, un servidor intermediario, cada servidor de aplicaciones proporciona servicios de datos a, al menos, un usuario usando al menos uno de los al menos un protocolos adicionales a través de al menos un servidor intermediario, un procedimiento de autenticación de al menos un equipo de usuario de acuerdo con la invención incluye el primer intermediario y al menos un intermediario adicional de al menos un servidor intermediario que autentica las solicitudes de los servicios de datos recibidas desde al menos un equipo de usuario de los protocolos usando la información de autenticación de al menos un perfil que se transmite desde el servidor de datos de abonado a, al menos, un servidor intermediario y la información de autenticación de al menos un usuario transmitida desde al menos un equipo de usuario a, al menos, un servidor intermediario y que proporciona información a, al menos, un servidor de aplicaciones permitiendo a, al menos, un usuario proporcionar la autorización final a, al menos, un usuario para acceder a, al menos, un servidor de aplicaciones o para proporcionar la autorización final de una acción que se realiza para al menos un usuario mediante al menos un servidor de aplicaciones. Al menos un servidor intermediario puede procesar la información de autenticación para proporcionar la información a, al menos, un servidor de aplicaciones para permitir a, al menos, un servidor de aplicaciones proporcionar la autorización final que incluye la garantía de la identidad de al menos un usuario. El procesamiento de la información de autenticación para proporcionar la información a, al menos, un servidor de aplicaciones puede comprender un secreto compartido conocido para, al menos, un servidor intermediario y al menos un servidor de aplicaciones que garantiza la identidad de al menos un usuario en al menos un servidor de aplicaciones. El secreto compartido puede ser un par de claves compartidas que se procesan mediante al menos un servidor de aplicaciones para verificar la identidad del usuario que va a recibir el acceso a, al menos, un servidor de aplicaciones o para quien al menos un servidor de aplicaciones toma la acción. El acoplamiento de al menos un servidor intermediario a, al menos, un servidor de aplicaciones puede ser a través de un medio seguro. Al menos un servidor de aplicaciones puede registrar los servicios de datos con al menos un servidor intermediario que al menos un servidor de aplicaciones puede proporcionar a, al menos, un usuario a través de al menos un servidor intermediario; y al menos un servidor intermediario puede almacenar una dirección de cada servidor de aplicaciones que proporciona los servicios de datos para su selección por al menos un usuario que se usa para conectar a, al menos, un usuario a, al menos, un servidor de aplicaciones para obtener los servicios de datos seleccionados. Al menos un servidor intermediario puede ser un punto de acceso en el sistema para la transmisión de los servicios de datos entre al menos un usuario y al menos un servidor intermediario.

Breve descripción de los dibujos

La figura 1 ilustra un diagrama de bloques de un sistema de acuerdo con la presente invención.

Mejor modo de llevar a cabo la invención

La figura 1 ilustra un sistema 10 que incluye entidades SIP convencionales. Las entidades incluyen al menos un UE 12, un S-CSCF 14 y un HSS 16. Al menos un servidor 18 intermediario tiene de manera residente, en el mismo, el P-CSCF 19 SIP, que se contacta mediante el UE 12, durante las sesiones que solicitan servicios de datos usando el protocolo SIP. Aunque se ilustra un único servidor 18 intermediario, debería entenderse que la invención puede ponerse en práctica con más de un servidor 18 intermediario, incluyendo intermediarios que usan información de autenticación transmitida desde el servidor de datos de abonado para autenticar las sesiones para múltiples protocolos. La autenticación de al menos un UE 12 por SIP y los protocolos adicionales usan el HSS 16 de la red 20 residencial que almacena, al menos, un perfil de usuario de los usuarios de al menos un UE con respecto a

proporcionar las sesiones de los servicios de datos. Se debería entender que el uso de SIP en la red 20 residencial como fuente de información de autenticación para los otros protocolos no se requiere en la práctica de la invención ya que la invención puede aplicarse a otros protocolos distintos de SIP. Al menos un perfil de usuario almacenado en el HSS 16 incluye la información de autenticación. Se usa la misma información de autenticación almacenada para autenticar a, al menos, un UE 12 de una sesión de servicios de datos cuando se hace una solicitud de los servicios de datos usando un primer protocolo, por ejemplo, sin limitación, el protocolo SIP y al menos un protocolo adicional.

Al menos un UE 12 solicita sesiones de servicios de datos usando el primer protocolo de red, por ejemplo, SIP y las sesiones de servicios de datos usando al menos un protocolo adicional. Al menos un UE 12 almacena información de autenticación para el primer protocolo que se transmite a, al menos, un servidor 18 intermediario para autenticar a, al menos, un UE 12 para todos los protocolos. El HSS 16, sin limitación, puede utilizar el protocolo AKA para proporcionar la información de autenticación en forma de las claves IK y CK, como se indica mediante la flecha 30 desde el HSS 16 a la P-CSCF 19 y el UE 12, en los que la información de autenticación se almacena y desde el UE a la P-CSCF, como se indica mediante la flecha 40.

La presente invención difiere de la técnica anterior en que al menos un servidor 18 intermediario incluye el P-CSCF 19 y el RSTP y los intermediarios 32 y 36 HTTP, respectivamente, para autenticar a, al menos, un UE 12 para usar al menos un protocolo, además del protocolo usado por la red residencial, por ejemplo, SIP, por ejemplo RTSP y HTTP. En una arquitectura preferida, se usa un único servidor 18 intermediario, pero la invención no se limita a ello. En una realización preferida, los servidores intermediarios adicionales son un intermediario 32 RTSP y un intermediario 36 HTTP todos los cuales están residentes en al menos un servidor 18 intermediario. La información de autenticación generada por SIP usada por al menos un UE 12 del intermediario 32 RTSP y del intermediario 36 HTTP es la misma que la usada por el P-CSCF 19.

De acuerdo con la invención, cuando al menos un UE 12 solicita una sesión de servicios de datos, tal como IMS, usando cualquier otro protocolo diferente del protocolo de la red 20 residencial, la solicitud se autentifica usando la información de autenticación proporcionada por la red residencial, por ejemplo, la información de autenticación SIP de IK y CK del HSS 16. Se debería entender que la invención no se limita al uso de la información de autenticación de IK y CK. Por lo tanto, si al menos un UE 12 solicita una sesión de servicios de datos usando un protocolo diferente al protocolo usado por la red 20 residencial, la información de autenticación obtenida a partir de un servidor de datos de abonado y específicamente, el HSS 16 del protocolo SIP se usa para al menos otro protocolo. Las solicitudes de servicios de datos para al menos un protocolo adicional, por ejemplo, los protocolos RTSP y HTTP se autentican usando la información de autenticación de la red 20 residencial almacenada en el servidor de datos de abonado de la red residencial, por ejemplo, el HSS 16.

El uso de al menos un servidor 18 intermediario para proporcionar autenticación para, al menos, un UE 12 que solicita sesiones que usan múltiples protocolos usando la información de autenticación de un solo protocolo usado en la red 20 residencial evita realizar la autenticación con la información única para cada uno de los protocolos como en la técnica anterior. Como resultado, se simplifica el requisito de la técnica anterior de proporcionar distinta información de autenticación para autenticar cada solicitud de una sesión de servicios de datos mediante al menos un UE 12 para cada protocolo adicional, ya que la autenticación del UE para usar los protocolos adicionales requiere el uso de, únicamente, la información de autenticación ya proporcionada desde el HSS 16 de la red 20 residencial del primer protocolo.

Una solicitud de una sesión de servicios de datos desde al menos un UE 12 se transmite al intermediario 32 RTSP del servidor 18 intermediario en el que al menos un UE 12 se autentifica y, posteriormente, se transmite al servidor 34 RTSP. De manera similar, una solicitud de una sesión de servicios de datos desde al menos un UE 12 se transmite al intermediario 36 HTTP del servidor 18 intermediario en el que al menos un UE 12 se autentifica y, posteriormente, se transmite al servidor 38 HTTP.

Los servidores 34 y 38 RTSP y HTTP están conectados al intermediario 32 RTSP y al intermediario 36 HTTP, respectivamente, de al menos un servidor 18 intermediario que son, preferentemente, conexiones seguras. Las conexiones seguras evitan los problemas de integridad de los mensajes y de los ataques hombre en el medio (man in the middle). Al menos un servidor 18 intermediario y, específicamente, el intermediario 32 RTSP y el intermediario 36 HTTP almacenan la dirección de cada servidor de aplicaciones asociado que, en general, se representa por el servidor 34 RTSP y el servidor 38 HTTP, respectivamente. El encaminamiento puede basarse en el direccionamiento que puede incorporar la información de dirección jerárquica en una URL tal como http.www.nokia.com/presence/user1 o la suma de una funcionalidad adicional a, al menos, un servidor 18 intermediario que se basa en bases de datos de contenido o de propiedad que contienen las direcciones de las aplicaciones ligadas al servidor intermediario. Esto puede implementarse de manera que al menos un servidor 18 intermediario actúa como un punto de entrada para un grupo de servidores de aplicaciones tales como, pero no limitado a los servidores 34 y 38 RTSP y HTTP, respectivamente. Al menos un servidor 18 intermediario puede procesar los paquetes de datos destinados a, al menos, un servidor de aplicaciones 34 y 38 para desprenderse de la carga y remitir la carga a través de las conexiones mencionadas anteriormente. Ejemplos de servidores de aplicaciones representados genéricamente por el servidor 38 HTTP identificado, sin limitación, son los servidores de presencia, mensajería y de conferencia usados, por ejemplo, para realizar tareas de gestión de servicios como la

manipulación de la política de autorización y la administración de la lista de miembros que funcionan de acuerdo con el protocolo HTTP. Algunos ejemplos de servidores de aplicaciones representados, genéricamente, por el servidor 34 RTSP identificado, sin limitación, son aplicaciones de transmisión de audio y vídeo en tiempo real.

Al menos un servidor 18 intermediario proporciona información de al menos un servidor 34 y 38 de aplicaciones permitiendo que al menos un servidor de aplicaciones proporcione la autorización final a, al menos, un usuario del UE 12 para acceder a, al menos, a un servidor de aplicaciones o proporcione la autorización final de una acción a realizarse por al menos un usuario mediante al menos un servidor de aplicaciones.

En una aplicación IMS, el servidor de aplicaciones realiza la mayor parte de la autorización del usuario del UE 12 para obtener el acceso o tener un servicio realizado por el UE. Al menos un servidor 18 intermediario autentica el mensaje de acuerdo con las especificaciones de IMS y algoritmos existentes, y pasa el resultado de la autorización a, al menos, un servidor 34 y 38 adicional. Al menos un servidor 34 y 38 adicional tiene el conocimiento último de los detalles específicos del servicio que están disponibles, en el mismo, para el usuario del UE 12 y la responsabilidad última de autorizar al usuario y/o a la acción a realizarse en el servidor específico. Al menos un servidor 34 y 38 adicional tiene la totalidad del conocimiento de la información específica del servicio y otra información para procesar el contenido recibido desde al menos un intermediario 18 a través del enlace seguro, preferentemente, para autorizar la acción intentada. El procedimiento de autorización último realizado por al menos un servidor 34 y 38 adicional se basa, preferentemente, en el intercambio de conocimiento secreto que puede ser, sin limitación, el uso de los pares de claves compartidas.

Aunque la invención se ha descrito en términos de sus realizaciones preferidas, debería entenderse que pueden hacerse numerosas modificaciones a la misma sin apartarse del alcance de la presente invención. Se pretende que todas estas modificaciones caigan dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un sistema (10) que comprende:

una red (20) residencial que incluye un servidor (16) de datos de abonado que está adaptado para almacenar al menos un perfil de usuario en lo concerniente a proporcionar servicios de datos a, al menos, un usuario con el perfil que incluye la información de autenticación usada para autenticar a, al menos, un usuario de los servicios de datos cuando se hace una solicitud de los servicios de datos usando un primer protocolo;
al menos un equipo (12) de usuario que está adaptado para solicitar servicios de datos usando el primer protocolo y servicios de datos usando al menos un protocolo adicional, al menos un equipo de usuario que almacena la información de autenticación que se usa cuando se hace una solicitud de servicios de datos para autenticar a, al menos, un usuario; y
al menos un servidor (18) intermediario que incluye de manera residente en el mismo, un primer intermediario (19) para el primer protocolo y al menos un intermediario (32, 36) adicional para el al menos un protocolo adicional, en el que
el primer intermediario (19) y el al menos un intermediario (32, 36) adicional del al menos un servidor (18) intermediario, están adaptados para autenticar las solicitudes de los servicios de datos recibidos desde al menos un equipo de usuario de los protocolos usando la información de autenticación del al menos un perfil que se transmite desde el servidor de datos de abonado a, al menos, un servidor intermediario y la información de autenticación del al menos un usuario transmitida desde el al menos un equipo de usuario a el al menos un servidor intermediario.

2. Un sistema de acuerdo con la reivindicación 1 en el que:

el servidor de datos de abonado es un servidor de abonado residencial (HSS); y
el primer protocolo es el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP se transmite desde una función de control del estado de la llamada de intermediario (P-CSCF) del al menos un servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial.

3. Un sistema de acuerdo con la reivindicación 1 en el que:

el servidor de datos de abonado es un servidor de abonado residencial (HSS);
el primer protocolo es el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP se transmite desde una función de control del estado de la llamada de intermediario (P-CSCF) del al menos un servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial; y
el al menos un protocolo adicional es el protocolo de transferencia de hipertexto (HTTP) y una solicitud de servicios de datos que usa HTTP se transmite desde un intermediario del protocolo de transferencia de hipertexto (HTTP) del al menos un servidor intermediario a un servidor HTTP.

4. Un sistema de acuerdo con la reivindicación 1 en el que:

el servidor de datos de abonado es un servidor de abonado residencial (HSS);
el primer protocolo es el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP se transmite desde una función de control del estado de la llamada de intermediario (P-CSCF) del al menos un servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF); y
el al menos un protocolo adicional es el protocolo de transmisión en tiempo real (RTSP) y una solicitud de servicios de datos se transmite desde un intermediario del protocolo de transmisión en tiempo real (RTSP) del al menos un servidor intermediario a un servidor RTSP.

5. Un sistema de acuerdo con la reivindicación 1 en el que:

el servidor de datos de abonado es un servidor de abonado residencial (HSS);
el primer protocolo es el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP se transmite desde una función de control del estado de la llamada de intermediario (P-CSCF) del al menos un servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial; y
el al menos un protocolo adicional es el protocolo de transferencia de hipertexto (HTTP) y el protocolo de transmisión en tiempo real (RTSP) y una solicitud de servicios de datos que usa HTTP se transmite desde un intermediario del protocolo de transferencia de hipertexto (HTTP) del al menos un servidor intermediario a un servidor HTTP y una solicitud de servicios de datos que usa RTSP se transmite desde el intermediario del protocolo de transmisión en tiempo real (RTSP) del al menos un servidor intermediario a un servidor RTSP.

6. Un sistema de acuerdo con las reivindicaciones 1-5 en el que:

la información de autenticación transmitida desde el servidor de datos de abonado al, al menos, un servidor intermediario comprende una clave de integridad IK y una clave de cifrado CK y la información de autenticación

transmitida desde el al menos un equipo de usuario al al menos un servidor intermediario comprende una clave de integridad IK y una clave de cifrado CK cuyas claves se procesan mediante el al menos un servidor intermediario para determinar si el al menos un usuario es auténtico.

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

la información de autenticación transmitida desde el servidor de datos de abonado y el al menos un equipo de usuario se genera usando el protocolo de acuerdo de autenticación y claves (AKA).

8. Un sistema de acuerdo con las reivindicaciones 1 a 7, que comprende además:

al menos un servidor (34, 38) de aplicaciones acoplado al, al menos, un servidor (18) intermediario, proporcionando cada servidor de aplicaciones servicios de datos al, al menos, un usuario usando al menos uno del al menos un protocolo adicional a través del al menos un servidor intermediario, en el que
el primer intermediario (19) y el al menos un intermediario (32, 36) adicional del al menos un servidor (18) intermediario están adaptados para proporcionar información al, al menos, un servidor de aplicaciones permitiendo al, al menos, un servidor de aplicaciones proporcionar la autorización final del, al menos, un usuario para acceder al, al menos, un servidor de aplicaciones o para proporcionar la autorización final de una acción a realizarse para al menos un usuario mediante el al menos un servidor de aplicaciones.

9. Un sistema de acuerdo con la reivindicación 8 en el que:

el al menos un servidor (18) intermediario está adaptado para procesar la información de autenticación para proporcionar la información al, al menos, un servidor de aplicaciones para permitir al, al menos, un servidor de aplicaciones proporcionar la autorización final que incluye la garantía de la identidad de al menos un usuario.

10. Un sistema de acuerdo con la reivindicación 9 en el que:

el procesamiento de la información de autenticación proporciona la información al, al menos, un servidor de aplicaciones que comprende, un secreto compartido conocido para el al menos un servidor intermediario y al, al menos, un servidor de aplicaciones que garantiza la identidad del al menos un usuario en el al menos un servidor de aplicaciones.

11. Un sistema de acuerdo con la reivindicación 10 en el que:

el secreto compartido es un par de claves compartidas que puede procesarse mediante el al menos un servidor de aplicaciones para verificar la identidad del usuario que va a recibir el acceso al, al menos, un servidor de aplicaciones o para quien al menos un servidor de aplicaciones toma la acción.

12. Un sistema de acuerdo con la reivindicación 8 en el que:

el acoplamiento del al menos un servidor intermediario a, al menos, un servidor de aplicaciones se realiza a través de un medio seguro.

13. Un sistema de acuerdo con la reivindicación 8 en el que:

el al menos un servidor (34, 38) de aplicaciones está adaptado para registrar servicios de datos con el al menos un servidor intermediario que al menos un servidor de aplicaciones puede proporcionar al, al menos, un usuario a través del al menos un servidor intermediario; y
el al menos un servidor (18) intermediario está adaptado para almacenar una dirección de cada servidor de aplicaciones que proporciona servicios de datos para su selección por el al menos un usuario que se usa para conectar el al menos un usuario al, al menos, un servidor de aplicaciones para obtener servicios de datos seleccionados.

14. Un sistema de acuerdo con la reivindicación 8 en el que:

el al menos un servidor (18) intermediario es un punto de acceso en el sistema para la transmisión de los servicios de datos entre el al menos un usuario y el al menos un servidor intermediario.

15. Un procedimiento de autenticación de al menos un equipo de usuario, que puede hacerse funcionar en un servidor (18) intermediario que incluye de manera residente en el mismo un primer intermediario (19) de un primer protocolo y al menos un intermediario (32, 36) adicional del al menos un protocolo adicional, que comprende:

recibir información de autenticación de al menos un perfil de usuario, que puede usarse para autenticar a, al menos, un usuario de los servicios de datos cuando se realiza una solicitud de los servicios de datos usando el primer protocolo, y que se transmite desde un servidor (16) de datos de abonado de una red (20) residencial que almacena al menos un perfil de usuario en lo concerniente a proporcionar servicios de datos al, al menos, un usuario,
recibir información de autenticación del al menos un usuario, que puede usarse cuando se hace una solicitud

de servicios de datos para autenticar al, al menos, un usuario, y que se transmite desde al menos un equipo (12) de usuario que solicita servicios de datos usando el primer protocolo y servicios de datos usando el al menos un protocolo adicional, y

autenticar, mediante el primer intermediario (19) y al menos un intermediario (32, 36) adicional del servidor (18) intermediario, las solicitudes de los servicios de datos recibidos desde el al menos un equipo de usuario de los protocolos usando la información de autenticación del al menos un perfil que se transmite desde el servidor de datos de abonado al servidor intermediario, y la información de autenticación de al menos un usuario transmitida desde al menos un equipo de usuario al servidor intermediario.

16. Un procedimiento de acuerdo con la reivindicación 15 en el que:

el servidor de datos de abonado es un servidor de abonado residencial (HSS); y

el primer protocolo es el protocolo de inicio de sesión (SIP) y cualquier solicitud de servicios de datos que usa SIP se transmite desde una función de control del estado de la llamada de intermediario (P-CSCF) del servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial.

17. Un procedimiento de acuerdo con la reivindicación 15 en el que:

el servidor de datos de abonado es un servidor de abonado residencial (HSS);

el primer protocolo es el protocolo de inicio de sesión (SIP) y una solicitud de datos de servicios de datos que usa SIP se transmite desde una función de control del estado de la llamada de intermediario (P-CSCF) del servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial; y

el al menos un protocolo adicional es el protocolo de transferencia de hipertexto (HTTP) y una solicitud de servicios de datos que usa HTTP se transmite desde un intermediario del protocolo de transferencia de hipertexto (HTTP) del servidor intermediario a un servidor HTTP.

18. Un procedimiento de acuerdo con la reivindicación 15 en el que:

el servidor de datos de abonado es un servidor de abonado residencial (HSS);

el primer protocolo es el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP se transmite desde una función de control del estado de la llamada de intermediario (P-CSCF) del servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF); y

el al menos un protocolo adicional es el protocolo de transmisión en tiempo real (RTSP) y una solicitud de servicios de datos se transmite desde un intermediario del protocolo de transmisión en tiempo real (RTSP) del servidor intermediario a un servidor RTSP.

19. Un procedimiento de acuerdo con la reivindicación 15 en el que:

el servidor de datos de abonado es un servidor de abonado residencial (HSS);

el primer protocolo es el protocolo de inicio de sesión (SIP) y una solicitud de datos de servicios de datos que usa SIP se transmite desde una función de control del estado de la llamada de intermediario (P-CSCF) del servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial; y

el al menos un protocolo adicional es el protocolo de transferencia de hipertexto (HTTP) y el protocolo de transmisión en tiempo real (RTSP) y una solicitud de servicios de datos que usa HTTP se transmite desde un intermediario del protocolo de transferencia de hipertexto (HTTP) del servidor intermediario a un servidor HTTP, y una solicitud de servicios de datos que usa RTSP se transmite desde un intermediario del protocolo de transmisión en tiempo real (RTSP) del servidor intermediario a un servidor RTSP.

20. Un procedimiento de acuerdo las reivindicaciones 15-19 en el que:

la información de autenticación transmitida desde el servidor de datos de abonado al servidor intermediario comprende una clave de integridad IK y una clave de cifrado CK y la información de autenticación transmitida desde el al menos un equipo de usuario al servidor intermediario comprende una clave de integridad IK y una clave de cifrado CK, claves se procesan mediante el servidor intermediario para determinar si al menos un usuario es auténtico.

21. Un procedimiento de acuerdo con la reivindicación 20 en el que:

la información de autenticación, transmitida desde el servidor de datos de abonado y el al menos un equipo de usuario, se genera usando el protocolo de acuerdo de autenticación y claves (AKA).

22. Un procedimiento de acuerdo con las reivindicaciones 15-21 que comprende además:

proporcionar información a, al menos, un servidor (34, 38) de aplicaciones, el al menos un servidor de aplicaciones está acoplado al, al menos, un servidor (18) intermediario, proporcionando cada servidor de

aplicaciones servicios de datos al, al menos, un usuario usando al menos uno de los al menos un protocolos adicionales a través del al menos un servidor intermediario, permitiendo al al menos un servidor de aplicaciones proporcionar autorización final al, al menos, un usuario para acceder al, al menos, un servidor de aplicaciones o para proporcionar autorización final de una acción a realizarse para el al menos un usuario mediante el al menos un servidor de aplicaciones.

23. Un procedimiento de acuerdo con la reivindicación 22 en el que:

el servidor intermediario procesa la información de autenticación para proporcionar la información al, al menos, un servidor de aplicaciones para permitir al menos un servidor de aplicaciones proporcionar la autorización final que incluye la garantía de la identidad del al menos un usuario.

24. Un procedimiento de acuerdo con la reivindicación 23 en el que:

el procesamiento de la información de autenticación para proporciona la información a , al menos, un servidor de aplicaciones que comprende un secreto compartido conocido para el servidor intermediario y el al menos un servidor de aplicaciones, que garantiza la identidad del al menos un usuario en el al menos un servidor de aplicaciones.

25. Un procedimiento de acuerdo con la reivindicación 24 en el que:

el secreto compartido es un par de claves compartidas que se procesa mediante el al menos un servidor de aplicaciones para verificar la identidad del usuario que va a recibir acceso al, al menos, un servidor de aplicaciones o para quien el al menos un servidor de aplicaciones toma la acción.

26. Un procedimiento de acuerdo con la reivindicación 25 en el que:

el acoplamiento del servidor intermediario al, al menos, un servidor de aplicaciones se realiza a través de un medio seguro.

27. Un procedimiento de acuerdo con la reivindicación 22 en el que:

el al menos un servidor de aplicaciones registra servicios de datos con el servidor intermediario que al menos un servidor de aplicaciones puede proporcionar al, al menos, un usuario a través del servidor intermediario; y
el servidor intermediario almacena una dirección de cada servidor de aplicaciones que proporciona los servicios de datos para su selección mediante al menos un usuario que se usa para conectar al, al menos, un usuario a, al menos, un servidor de aplicaciones para obtener los servicios de datos seleccionados.

28. Un procedimiento de acuerdo con la reivindicación 22 en el que:

el servidor intermediario es un punto de acceso en el sistema para la transmisión de los servicios de datos entre el al menos un usuario y el servidor intermediario.

29. Un servidor (18) intermediario que comprende:

un primer intermediario (19) de un primer protocolo y al menos un intermediario (32, 36) adicional de al menos un protocolo adicional que está de manera residente en el mismo, en el que
el servidor (18) intermediario está adaptado para recibir información de autenticación de al menos un perfil de usuario, que puede usarse para autenticar al menos un usuario de los servicios de datos cuando se hace una solicitud de los servicios de datos usando un primer protocolo, y que se transmite desde un servidor (16) de datos de abonado de una red (20) residencial que almacena el al menos un perfil de usuario en lo concerniente a proporcionar servicios de datos al, al menos, un usuario,
el servidor (18) intermediario está adaptado para recibir información de autenticación del al menos un usuario, que puede usarse cuando se hace una solicitud de servicios de datos para autenticar al, al menos, un usuario, y que se transmite desde el al menos un equipo (12) de usuario que solicita servicios de datos usando el primer protocolo y los servicios de datos usando al menos un protocolo adicional, y
el primer intermediario (19) y el al menos un intermediario (32, 36) adicional, están adaptados para autenticar las solicitudes de servicios de datos recibidas desde el al menos un equipo de usuario de los protocolos usando la información de autenticación de al menos un perfil que se transmite desde el servidor de datos de abonado al servidor intermediario, y la información de autenticación del al menos un usuario transmitida desde el al menos un equipo de usuario al servidor intermediario.

30. Un servidor intermediario de acuerdo con la reivindicación 29 en el que:

el servidor de datos de abonado es un servidor de abonado residencial (HSS); y
el primer protocolo es el protocolo de inicio de sesión (SIP) y cualquier solicitud de servicios de datos que usa SIP se transmite desde una función de control del estado de la llamada de intermediario (P-CSCF) del servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial.

31. Un servidor intermediario de acuerdo con la reivindicación 29 en el que:

el servidor de datos de abonado es un servidor de abonado residencial (HSS); y
el primer protocolo es el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP se transmite desde una función de control del estado de la llamada de intermediario (P-CSCF) del servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial; y el al menos un protocolo adicional es el protocolo de transferencia de hipertexto (HTTP) y una solicitud de servicios de datos que usa HTTP se transmite desde un intermediario del protocolo de transferencia de hipertexto (HTTP) del servidor intermediario a un servidor HTTP.

32. Un servidor intermediario de acuerdo con la reivindicación 29 en el que:

el servidor de datos de abonado es un servidor de abonado residencial (HSS); y
el primer protocolo es el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP se transmite desde el servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF), y el al menos un protocolo adicional es el protocolo de transmisión en tiempo real (RTSP) y una solicitud de servicios de datos se transmite desde un intermediario del protocolo de transmisión en tiempo real (RTSP) del servidor intermediario a un servidor RTSP.

33. Un servidor intermediario de acuerdo con la reivindicación 29 en el que:

el servidor de datos de abonado es un servidor de abonado residencial (HSS); y
el primer protocolo es el protocolo de inicio de sesión (SIP) y una solicitud de servicios de datos que usa SIP se transmite desde una función de control del estado de la llamada de intermediario (P-CSCF) del servidor intermediario a un servidor de la función de control del estado de la llamada de servicio (S-CSCF) de la red residencial, y el al menos un protocolo adicional es el protocolo de transferencia de hipertexto (HTTP) y el protocolo de transmisión en tiempo real (RTSP) y una solicitud de servicios de datos que usa HTTP se transmite desde un intermediario del protocolo de transferencia de hipertexto (HTTP) del servidor intermediario a un servidor HTTP y una solicitud de servicios de datos que usa RTSP se transmite desde un intermediario del protocolo de transmisión en tiempo real (RTSP) del servidor intermediario a un servidor RTSP.

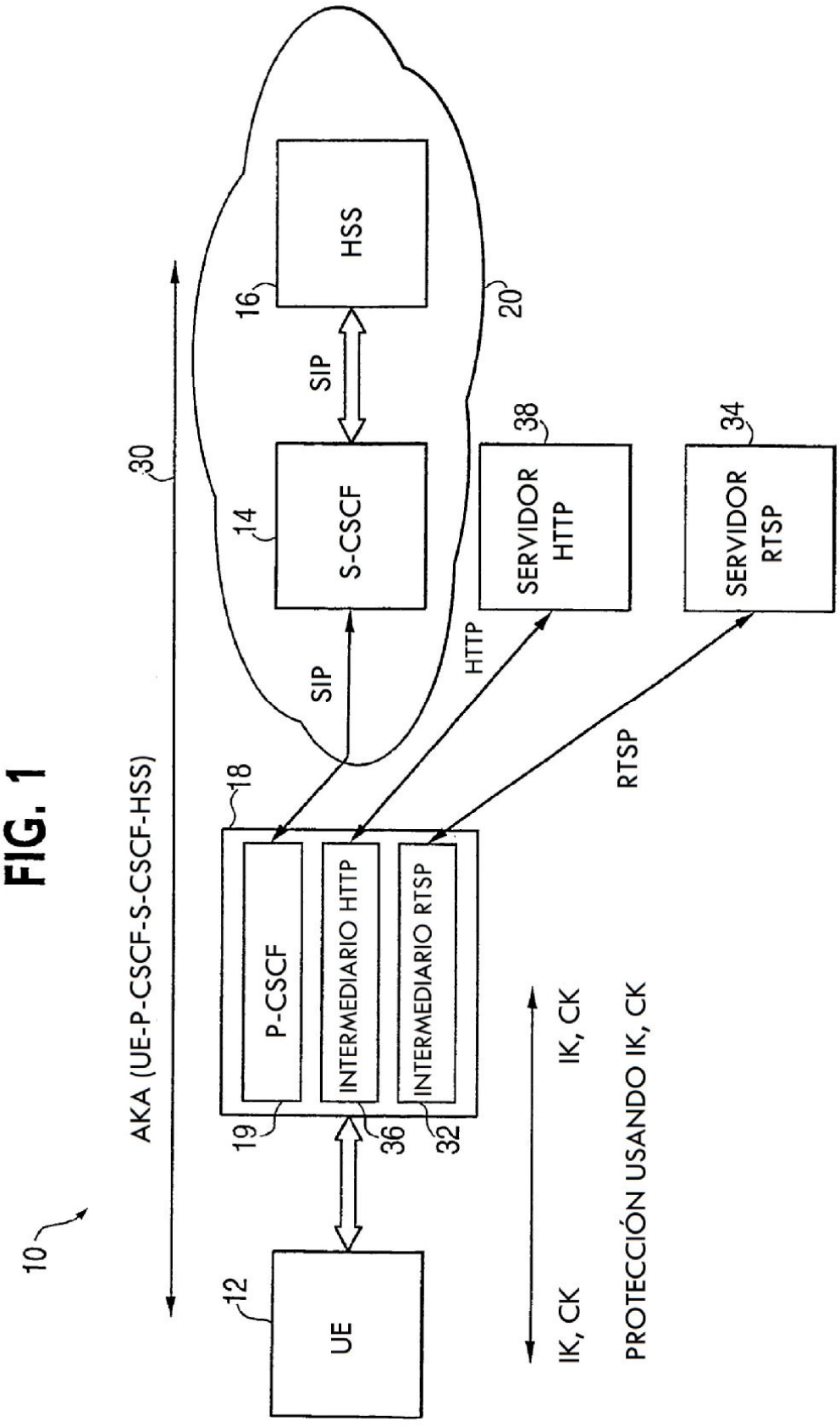
34. Un servidor intermediario de acuerdo con las reivindicaciones 29-33 en el que:

la información de autenticación transmitida desde el servidor de datos de abonado al servidor intermediario comprende una clave de integridad IK y una clave de cifrado CK y la información de autenticación transmitida desde el al menos un equipo de usuario al servidor intermediario comprende una clave de integridad IK y una clave de cifrado CK, claves que se procesan mediante el servidor intermediario para determinar si el al menos un usuario es auténtico.

35. Un servidor intermediario de acuerdo con la reivindicación 34 en el que:

la información de autenticación transmitida desde el servidor de datos de abonado y el al menos un equipo de usuario se genera usando el protocolo de acuerdo de autenticación y claves (AKA).

FIG. 1


10
12
UE
AKA (UE-P-CSCF-S-CSCF-HSS)
30
18
P-CSCF
INTERMEDIARIO HTTP
INTERMEDIARIO RTSP
19
36
32
SIP
14
S-CSCF
16
HSS
20
HTTP
SERVIDOR HTTP
38
RTSP
SERVIDOR RTSP
34
IK, CK
IK, CK
PROTECCIÓN USANDO IK, CK