(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 769 528**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
G06F 21/33 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.06.2005 PCT/IB2005/002035**

(87) Fecha y número de publicación internacional: **12.01.2006 WO06003499**

(96) Fecha de presentación y número de la solicitud europea: **24.06.2005 E 05759785 (8)**

(97) Fecha y número de publicación de la concesión europea: **16.10.2019 EP 1763947**

(54) Título: **Autentificación de usuarios**

(30) Prioridad:

28.06.2004 GB 0414421

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.06.2020

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karakaari 7
02610 Espoo, FI

(72) Inventor/es:

MONONEN, RISTO;
ASOKAN, NADARAJAH y
LAITINEN, PEKKA

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Autentificación de usuarios

Campo de la invención

La presente invención se refiere a la autentificación de usuarios, particularmente en el contexto de proporcionar servicios a los usuarios (suscriptores) de una red de comunicaciones inalámbricas.

Antecedentes de la invención

Una forma de mantener la privacidad del usuario es que un usuario proporcione diferentes identidades a diferentes proveedores de servicios. Estas identidades se denominan en el presente documento identidades específicas del servicio. En tal caso, sin embargo, es necesario que el operador de una red para los suscriptores proporcione un servicio de gestión de identidad que pueda asociar identidades específicas del servicio con suscriptores autorizados. También es útil si un proveedor de gestión de identidad puede hacer autorizaciones no solo en nombre de sí mismo, sino también en nombre de otros proveedores de servicios. Esto significa que los usuarios pueden invocar servicios personalizados sin tener que iniciar sesión por separado en cada sitio de perfil de servicio.

Esta disposición se conoce como federación de identidad y permite a los proveedores de servicios leer la identidad de un usuario desde un lugar centralizado. Un usuario no tiene que proporcionar a todos los proveedores de servicios información de identidad específica.

Actualmente hay dos métodos de autentificación significativos especificados para redes de comunicación inalámbricas en las que un equipo de usuario (UE) en forma de terminal móvil desea acceder a un servicio desde un proveedor de servicios en la red. El llamado estándar Liberty Alliance (LA) utiliza un método de autentificación en el que un cliente con libertad habilitada (LEC) es un cliente que tiene, o sabe cómo obtener, conocimiento sobre el proveedor de identidad que el usuario desea usar con el proveedor de servicios. Especifica la asignación de identidad específica del servicio en un proveedor de identidad (IDP). Cada suscriptor tiene múltiples identidades para acceder a los proveedores de servicios (SP). Un directorio de federación en el proveedor de identidad almacena las relaciones entre usuarios, sus identidades y los servicios. El proveedor de identidad afirma una identidad específica del servicio hacia el proveedor del servicio que reconoce al usuario por esa identidad específica del servicio. La capacidad de presentar diferentes identidades a diferentes proveedores de servicios permite mantener la privacidad del suscriptor. De acuerdo con el estándar de Liberty Alliance, el usuario puede evitar revelar su identidad real al invocar servicios. En lugar de revelar su verdadera identidad, el usuario puede invocar los servicios de forma anónima o usar un seudónimo (una identidad específica del servicio). El directorio de la federación asigna la identidad real del usuario a sus seudónimos o identidades específicas del servicio para que el proveedor del servicio no conozca la identidad real. Con el seudónimo y el servicio de mapeo, el proveedor de servicios puede acceder a, por ejemplo, la ubicación del usuario o el estado de presencia. Esto permite que un proveedor de servicios use el seudónimo para acceder a la ubicación del usuario desde un proveedor de servicios de identidad a través de la asignación en la base de datos de la federación. El estándar Liberty Alliance especifica el enlace HTTP/soap firmado que se utilizará para las aserciones. Sin embargo, existen muchos servicios existentes que no conocen las afirmaciones de Liberty pero dependen de otras formas de "aserciones" para acceder, como los certificados de clave pública tradicionales. Un ejemplo de dicho servicio es el control de acceso a redes privadas virtuales (VPN) corporativas.

Otra forma de autentificación existente es el soporte 3GPP para certificados de suscriptor (SSC) [3GPP TS 33.221]. Esto se implementa como una arquitectura de autentificación genérica (GAA) 3GPP [3GPP TS 33.220] y especifica una forma de solicitar un certificado de suscriptor para una identidad específica de la autoridad de certificación (CA). En este caso, la identidad específica es la identidad del usuario y no es específica del servicio. De acuerdo con la técnica GAA/SSC, la arquitectura de arranque genérico (GBA) implantada en el equipo del usuario autentifica el equipo del usuario junto con un servidor de autentificación en el proveedor de servicios, y acuerdan un material de clave compartida. La arquitectura de arranque genérico entrega el material de clave compartida a una autoridad de certificación CA. Los equipos de usuario generan un par de claves públicas/privadas asimétricas y solicitan la certificación de la autoridad de certificación. Si está autorizado, se devuelve un certificado que asocia la clave pública con la identidad del usuario solicitante. El método de certificación está protegido por el material de clave compartida. El lenguaje de federación de servicios web (Federación WS), versión 1.0, del 8 de julio de 2003 divulga un sistema en el que un solicitante puede solicitar a un proveedor de identidad una señal a un campo de confianza. El proveedor de identidad busca un seudónimo y emite una señal que se puede utilizar en un recurso específico.

Los operadores móviles pueden autentificar a sus suscriptores móviles utilizando USIM, ISIM, par de nombre de usuario/contraseña o certificados de clave pública X.509. En el caso de los certificados, la identidad autentificada está en el campo nombreSujeto o en la extensión NombreAltSujeto del certificado [RFC 3280].

El método de autentificación 3GPP/GAA/SSC no tiene un mecanismo para indicar el proveedor de servicios al que desea acceder el suscriptor. Solo la identidad del usuario puede ser indicada y autentificada por el certificado. No

hay soporte para la autentificación basada en certificados de múltiples identidades o identidades específicas del servicio. Aunque la extensión NombreAltSujeto se puede usar para transportar múltiples identidades e identidades específicas del servicio, el problema es que el equipo del usuario debe poder indicar durante el método de certificación la identidad o identidades previstas, es decir, servicio o servicios con los que planea usar el certificado. No quiere poner todas las identidades posibles en un solo certificado, porque descubrir los enlaces entre diferentes identidades sería muy fácil, ya que el certificado es público.

Sumario de la invención

Es un objetivo de la presente invención proporcionar un sistema de autentificación que no esté sujeto a los límites de los dos sistemas descritos anteriormente.

De acuerdo con un aspecto de la invención, se proporciona un método para autentificar un terminal de usuario que busca acceso a un servicio de un proveedor de servicios en una red de comunicación, comprendiendo el método: asignar al terminal de usuario una pluralidad de identidades específicas de servicio para acceder a servicios respectivos; emitir una solicitud desde el terminal de usuario, identificando la solicitud el servicio al que se accede y que incluye una clave pública del terminal de usuario; en una autoridad de certificación, autentificar la solicitud y emitir un certificado de clave pública para vincular la identidad específica del servicio con la clave pública en la solicitud y devolver el certificado de clave pública al terminal de usuario.

En la siguiente realización descrita, la solicitud incluye un identificador de servicio que identifica el servicio al que se va a acceder y un identificador de solicitante que identifica el terminal de usuario. El método comprende la etapa adicional de, en la autoridad de certificación, mapear el identificador de servicio, emparejar el identificador del solicitante con la identidad específica del servicio que se autentificará. Sin embargo, también es posible implementar la invención cuando la solicitud identifica la identidad específica del servicio y en el que el método comprende la etapa adicional de la autoridad de certificación que verifica que el terminal de usuario está autorizado para usar la identidad específica de servicio.

En un ejemplo, la etapa de emisión comprende emitir la solicitud que comprende un mensaje que incluye una pluralidad de campos, conteniendo uno de dichos campos un identificador de servicio para identificar el servicio al que se accede. En un ejemplo, el campo que contiene el identificador de servicio es un campo sujeto. En un ejemplo, la etapa de emisión comprende emitir la solicitud que comprende un mensaje PKCS#10. En un ejemplo, la etapa de emisión comprende emitir la solicitud que comprende un mensaje CRMF. En un ejemplo, la etapa de emisión comprende emitir la solicitud que comprende un mensaje HTTP. En un ejemplo, el método comprende implementar las etapas de asignación, emisión, autentificación y devolución en una red de comunicaciones inalámbricas.

La invención es particularmente útil en el contexto de redes de comunicaciones inalámbricas, aunque se apreciará que la invención también es aplicable a otros tipos de redes de comunicación.

Otro aspecto de la invención proporcionó un terminal de usuario para el usuario en una red de comunicaciones que comprende: medios para emitir una solicitud que identifica un servicio al que se accede a través de la red de comunicaciones inalámbricas e incluye una clave pública; medios para recibir un certificado de clave pública emitido por una autoridad de certificación que asocia una identidad específica del servicio para acceder al servicio con la clave pública; y medios para reenviar el certificado de clave pública a un proveedor de servicios para autentificar la identidad específica del servicio para el terminal de usuario y autorizar así el acceso al servicio.
En un ejemplo, el terminal de usuario comprende medios para establecer material de clave compartida con la autoridad de certificación antes de emitir la solicitud. En un ejemplo, el terminal de usuario comprende medios para generar un par de claves asimétricas que incluyen la clave pública y una clave privada. En un ejemplo, el terminal de usuario comprende medios para emitir dicha solicitud a través de una interfaz inalámbrica. En un ejemplo, la solicitud identifica el servicio utilizando al menos uno de: una cadena transparente; una dirección de campo, un identificador universal de recursos; un nombre distinguido. En un ejemplo, la identidad específica del servicio no está incluida en la solicitud.

Un aspecto adicional de la invención proporciona un sistema de autentificación para usar en una red de comunicaciones para permitir el acceso a un servicio desde un proveedor de servicios, comprendiendo el sistema: una autoridad de certificación que comprende medios para recibir una solicitud de un terminal de usuario, identificando la solicitud el servicio al que se accede y que incluye una clave pública del terminal de usuario; y en el que la autoridad de certificación está dispuesta para autentificar la solicitud y emitir un certificado de clave pública para una identidad específica del servicio a la que se accederá y devolver el certificado de clave pública al terminal de usuario.
En un ejemplo, el sistema de autentificación comprende un servidor de autentificación configurado para autentificar la identidad del terminal de usuario que emite la solicitud. En un ejemplo, la autoridad de certificación comprende una base de datos de federación, configurándose la base de datos de federación para asignar el servicio y los identificadores del solicitante a las identidades específicas del servicio para acceder a servicios respectivos. En un ejemplo, los medios para recibir dicha solicitud comprenden medios para recibir dicha solicitud a través de una

interfaz inalámbrica.

Para una mejor comprensión de la presente invención y para mostrar cómo la misma puede llevarse a efecto, se hará ahora referencia, a modo de ejemplo, a los dibujos adjuntos.

Breve descripción de los dibujos

La figura 1 es un diagrama esquemático que muestra una red de comunicaciones donde un suscriptor puede acceder a uno o más servicios;

La figura 2 ilustra una arquitectura de ejemplo para implementar una realización de la invención;

La figura 3 es un diagrama esquemático de un directorio de federación;

La figura 4 ilustra el flujo de mensajes entre el suscriptor y el servidor de autentificación; y

La figura 5 ilustra el flujo de mensajes entre el suscriptor y la autoridad de certificación.

Descripción de las realizaciones preferidas

La figura 1 es un diagrama de bloques esquemático de una red de comunicaciones inalámbricas para proporcionar servicios a un suscriptor. El suscriptor se indica en forma de un equipo de usuario (UE), que puede ser un terminal móvil tal como un teléfono móvil, ordenador personal o cualquier otro tipo de dispositivo de comunicación móvil. El equipo de usuario UE tiene un circuito de recepción/transmisión 50 que es capaz de recibir y transmitir datos, tal como mensajes de solicitud y respuesta, a la red a través de un enlace de radio RL capaz de soportar comunicaciones inalámbricas. El equipo de usuario UE también incluye una memoria 52 para contener información de autentificación como se describe con más detalle a continuación. El terminal móvil es capaz de ejecutar software de cliente como se describe con más detalle a continuación. El UE del suscriptor se comunica con varios proveedores de servicios diferentes SP1, SP2...SPN a través de una red de operador. La red incluye o tiene acceso a un subsistema de autorización 26 que actúa como un proveedor de identidad centralizado para los proveedores de servicios que acceden a la red. Un suscriptor que desee acceder a un servicio será autorizado en función de su identidad autentificada.

La figura 2 ilustra una arquitectura de ejemplo para implementar una realización de la presente invención. Ilustra una arquitectura de autentificación genérica (GAA) que incluye un cliente 4 de arquitectura de arranque genérico (GBA) ejecutado en el terminal móvil conectado a un servidor de autentificación (función de servidor de arranque - BSF) a través de una interfaz Ub. El servidor de autentificación 6 está conectado a un servidor de suscriptor doméstico (HSS)/registro de ubicación de origen (HLR) 8, que almacena datos de autentificación, incluyendo claves K y la identidad internacional del suscriptor móvil (IMSI) para los suscriptores. El servidor de autentificación 6 está conectado a una autoridad de certificación (CA) 10 a través de una interfaz Zn. La autoridad de certificación 10 incluye un directorio de federación. El directorio de federación (FD) se ilustra en la figura 3. Asocia cada identidad de suscriptor con una pluralidad de identidades específicas de servicio (SSI) que el suscriptor utiliza como su cara para acceder a diferentes servicios de los proveedores de servicios. La identidad del suscriptor en el directorio de federación es el nombre de usuario por el cual la red del operador conoce al suscriptor. El número de referencia 12 indica un dominio de certificado de clave pública PKC. El dominio de certificado de clave pública 12 comprende un cliente de certificación 14 (ejecutado en el terminal móvil que está conectado al cliente de autorización 4 a través de una interfaz PK, y a la autoridad de certificación 10 a través de una interfaz Ua. El dominio de certificado de clave pública 12 también incluye una función de puerta de enlace de seguridad (Seguridad de la capa de transporte) SEC (TLS) 16 que está conectada al cliente de certificación 14 a través de una interfaz PK1. La puerta de enlace SEC (TLS) 16 es parte del servidor HTTP que realiza la parte de autentificación TLS en nombre del servidor HTTP.

Debe tenerse en cuenta que en la siguiente descripción, el ejemplo que se proporciona se implementa con servicios basados en http. Sin embargo, el principio subyacente se puede utilizar para IPSec (seguridad de protocolo de Internet), VPN (redes privadas virtuales) o WLAN (redes inalámbricas de área local) también.

El número de referencia 18 indica un dominio http que comprende un cliente http 20, por ejemplo, en forma de navegador, que está conectado al cliente de certificación 14 del dominio PKC a través de una interfaz HT3 y al cliente de autorización del dominio GAA a través de una interfaz TE-AA. El cliente http 20 está conectado a un clasificador http 22 a través de una interfaz HT1. El clasificador http está conectado a una función de servidor http 24 a través de una interfaz HT4. El clasificador http 22 está conectado al cliente de certificación del dominio PKC a través de una interfaz HT2. La función de servidor http 24 está conectada a la función de puerta de enlace SEC (TLS) 16 del dominio PKC a través de una interfaz interna SP-AA. El cliente http y el clasificador se ejecutan en el terminal móvil UE. La función del servidor http 24 está asociada con uno de los proveedores de servicios SP de la figura 1.

Volviendo al dominio GAA 2, el cliente de autentificación GBA 4 en el equipo de usuario UE se autentifica en el

servidor BSF, y acuerdan un material de clave compartida. El servidor BSF 6 se usa para autentificar el equipo del usuario utilizando el protocolo de autentificación con resumen HTTP y acuerdo de clave (AKA) especificado en la solicitud de comentarios (RFC) 3310, dando como resultado un material clave compartido entre el servidor BSF 6 y el equipo de usuario UE. El servidor BSF 6 interactúa con el servidor de abonado doméstico/registro de ubicación de inicio 8 para obtener la información de autentificación correspondiente, en forma de autentificación de triplete/vectores. La autoridad de certificación 10 actúa como un portal PKI y puede emitir un certificado para el equipo del usuario y entregar un certificado de CA de operador. En ambos casos, las solicitudes y respuestas están protegidas por el material de clave compartida que se ha establecido previamente entre el equipo del usuario y el servidor de autorización.

Ahora se describirá un método de acuerdo con una realización de la invención para permitir que un suscriptor que usa el equipo de usuario UE acceda a un servicio proporcionado por uno de los proveedores de servicios SP. El cliente GBA 4 se comunica con el servidor de autentificación BSF para autentificar al suscriptor en función de su identidad de suscriptor (por ejemplo, nombre de usuario) y para acordar un material de clave compartida K_s. El material de clave compartida se deriva de la información de autentificación tanto en el cliente de autorización 4 como en la autoridad de certificación 10. El cliente 4 deriva el material de clave compartida Ks con el protocolo HTTP con resumen AKA que requiere una clave secreta y una función criptográfica para destilar el material de clave compartida Ks del desafío de autentificación. El material de clave compartida se mantiene en el directorio de federación FD en asociación con la identidad de suscriptor relacionada para esta sesión autentificada. El material de clave compartida toma la forma de un código de cifrado.

El equipo de usuario UE genera entonces un par de clave pública/clave privada y los almacena con un identificador de servicio SI_i que identifica el servicio al que desea acceder el suscriptor. Se pueden almacenar en la memoria 52 en el equipo del usuario o en una tarjeta inteligente accesible por el equipo del usuario.

Se invoca al cliente de certificación 14 para solicitar un certificado. Una solicitud incluye el identificador de servicio y la clave pública: la clave privada se mantiene en secreto. La solicitud del certificado está protegida con el material de clave compartida y se transmite a través de la interfaz Ua a la autoridad de certificación CA. La identidad del suscriptor también se transmite con la solicitud.

En la autoridad de certificación 10, el directorio de federación FD asigna el identificador de servicio SI_i a la identidad específica de servicio SSI_i para ese servicio y ese nombre de usuario.

La autoridad de certificación 10 obtiene el material de clave compartida K_{si} basado en el nombre de usuario del servidor BSF 6 y verifica el encabezado de autorización de la solicitud. Esto se discute en TS 33.221. Suponiendo que la solicitud es válida, la autoridad de certificación 10 emite un certificado que asocia la clave pública con la identidad específica del servicio para el servicio identificado por el identificador de servicio en la solicitud. El certificado se devuelve al suscriptor UE a través de la interfaz Ua, y el UE lo almacena en la memoria 52 o tarjeta inteligente. En el caso de múltiples dispositivos, el UE puede reenviar el certificado a otro dispositivo (ordenador portátil) posiblemente con la clave privada a menos que el otro dispositivo haya generado la clave privada.

El cliente de certificación 14 avisa al cliente http 20 sobre la interfaz HT3 que se ha recibido un certificado válido y reenvía el certificado para la autentificación a la función de puerta de enlace SEC (TLS) 16 a través de la interfaz PK1. El cliente http 20 invoca entonces la función 24 del servidor http del proveedor de servicios para el servicio al que desea acceder e incluye el certificado. También incluye evidencia por la cual el proveedor de servicios puede validar el certificado, incluyendo, por ejemplo, una firma digital que comprende datos cifrados con la clave privada.

La puerta de enlace SEC (TLS) 16 valida el certificado a través de la interfaz PK3 contra una lista de autoridades de certificación y, una vez que el certificado ha sido autentificado, se puede invocar el servicio para el suscriptor. La función de puerta de enlace SEC (TLS) 16 también desafía al cliente y verifica la respuesta para autentificar al cliente (PK1), y hace que la función 24 del servidor http brinde el servicio solicitado a los clientes autorizados (HT4).

La autentificación a través de la interfaz Ub se lleva a cabo de acuerdo con los estándares 3GGP TS 33.220, con la autentificación realizada basándose en HTTP con resumen AKA [RFC 3310], La autentificación también podría llevarse a cabo utilizando SIM 2G.

La figura 4 muestra parte del flujo de mensajes entre el equipo de usuario UE que implementa el cliente de autorización 4 (UE) y el servidor de autorización 6 (BSF) durante el método de arranque. El cliente GBA 4 inicia un método de autentificación emitiendo una solicitud de autentificación 30 de solicitud GET. La solicitud de autentificación identifica al usuario utilizando la identidad del suscriptor; en este ejemplo es la IMPI (identidad privada multimedia IP). La otra alternativa podría ser IMSI, o el UE podría generar un pseudo IMPI a partir del IMSI (como se especifica en TS 23.003). Se devuelve una respuesta HTTP 32 que reconoce la identidad de usuario IMPI y devuelve una palabra que contiene RAND y AUTN de AKA que identifica de forma exclusiva la solicitud. El cliente de autentificación 4 en el equipo de usuario devuelve una solicitud HTTP 34 con una contraseña adecuada derivada de AKA, y el servidor de autorización (BSF) 6 responde devolviendo información de autentificación que incluye el identificador de transacción de arranque (B-TID) (no se muestra en la figura 4) que se utiliza como nombre de

usuario en la interfaz Ua, y el material de clave compartida se deriva de la información de autentificación. Quedará claro que el BSF ha accedido a la información de autentificación desde el HSS, pero esta interacción no se muestra en la figura 2 porque ya se conoce.

Después de que el material clave compartido haya sido acordado por el intercambio de mensajes de la figura 4, entonces el cliente de certificación en el equipo del usuario genera una solicitud de certificación PKCS#10 que se transfiere a través de la interfaz Ua a la CA. Esto se muestra en la figura 5. La solicitud de certificación incluye varios campos de acuerdo con el estándar establecido de la siguiente manera:

```
POST /certificaterequest/ HTTP/1.1
Authorization: Digest
username="adf..adf",
realm="ca-naf@operator.com",
qop="auth-int",
algorithm="MD5",
uri="/certificaterequest/",
nonce="dffef12..2ff7",
nc=00000001,
cnonce="0a4fee..dd2f'',
response="6629..af3e",
opaque="e23f45..dff2"

<base64 encoded PKCS#10 request>
```

Los campos se conocen por RFC 2617. En este ejemplo, el mensaje HTTP contiene un encabezado HTTP de Autorización donde el "nombre de usuario" podría ser B-TID, y el campo "opaco" puede incluir identificadores de servicio.

La "Autorización" es el encabezado HTTP asociado con la autentificación HTTP con resumen [RFC 2617]. Los parámetros en el encabezado de autorización se utilizan para autentificar y proteger la integridad de la solicitud. La solicitud PKCS#10 contiene la propia solicitud de certificación, incluyendo la clave pública del usuario y el identificador del servicio.

De acuerdo con una realización de la invención, la solicitud de certificación PKCS#10 también incluye un campo de identificador de servicio que identifica el servicio al que debe acceder el usuario. El servicio se puede identificar de varias maneras, por ejemplo, mediante una cadena transparente, una dirección de campo, un URI (identificador universal de recursos), un nombre distinguido, etc. Todo lo que se necesita es el identificador único para el servicio particular al que debe acceder el usuario. El identificador de servicio se incluye en la solicitud PKCS#10, como una de las extensiones. Como un ejemplo, hay un atributo "Solicitud de extensión" en PKCS#9 que se puede usar con PKCS#10, con NombreAltsujeto como la extensión solicitada.

Alternativamente, en CRMF (Formato de mensaje de solicitud de certificado) [RFC 2511] podría ser la extensión NombreAltsujeto en el campo de plantilla de certificado (PlantillaCert).

La CA(NAF) obtiene el material de clave compartida del servidor de autorización BSF basado en el nombre de usuario (B-TID) suministrado en la solicitud de certificación PKCS#10 y verifica el encabezado de autorización utilizando el material de clave compartida. Si tiene éxito, procesa la solicitud de certificación y devuelve una respuesta de certificado etiquetada CERT en la figura 5. La respuesta del certificado tiene el siguiente formato:

```
HTTP/1.1 200 OK
Content Type: application/x509-user-cert
Authentication-info:nextnonce="4ff232dd...dd"
qop=auth-int
rspauth="4dd34...55d2"
cnonce="0a4fee...dd2f''
nc=00000001

<base 64 encoded subscriber x509 certificate>
```

El equipo de usuario almacena el certificado en el equipo de usuario en la memoria o tarjeta inteligente. El certificado activa la clave pública con el identificador de servicio y puede autentificarse utilizando el par asimétrico de clave pública/clave privada.

Al agregar el identificador de servicio a la solicitud de certificación, esto permite a los suscriptores tener múltiples certificados para múltiples servicios. Sin embargo, el usuario puede retener una identidad única para cada servicio porque cada certificado de suscriptor está asociado con una identidad de suscriptor específica de un servicio en

particular, en lugar de con una identidad común ("global") cuya actividad podría rastrearse, violando la privacidad del suscriptor. En otras palabras, hemos reemplazado las afirmaciones de Liberty Alliance específicas del suscriptor y del servicio con certificados de clave pública específicos del suscriptor y del servicio. En la realización descrita anteriormente, la CA identifica la identidad de usuario específica del servicio en función del material de clave compartida y la asignación que se mantiene en la base de datos de la federación.

En una realización alternativa, el equipo de usuario UE podría enviar una solicitud de certificación indicando su identidad preferida, por ejemplo, en el caso de que un suscriptor tenga varios nombres para acceder a un proveedor de servicios.

En la CA (o en el directorio de la federación), el par (identificador de solicitante, identificador de servicio) se asigna a una identidad de abonado específica del servicio que se mantiene en la base de datos de la federación. La autoridad de certificación firma el certificado de clave pública para la identidad asignada y lo devuelve al equipo del usuario.

Esto permite a los suscriptores tener múltiples identidades en múltiples certificados. Las claves públicas en los certificados deben diferir para evitar vincular las identidades. Por lo tanto, la realización de la invención descrita anteriormente admite los estándares de privacidad de Liberty Alliance (LA) mediante el mapeo de identidad con la tecnología de certificado de clave pública, pero puede alcanzar una gama más amplia de aplicaciones que el mecanismo de afirmación de LA.

En la realización descrita anteriormente, el identificador de servicio se incluye en un campo de extensión adicional en el mensaje PKCS#10. El identificador de servicio se asigna a una identidad específica de servicio en la base de datos de federación FD asociada con la autoridad de certificación CA.

De acuerdo con una primera realización alternativa, es posible enviar la identidad específica del servicio en la solicitud de certificación. Es decir, el UE mismo asigna la identidad del suscriptor a la identidad específica del servicio deseada para el certificado. En ese caso, la autoridad de certificación debe verificar que el suscriptor en cuestión posee realmente la identidad solicitada y debe mantener una base de datos de identidad para esa verificación. Por lo tanto, la arquitectura resultante es más compleja que la realización descrita anteriormente, pero el protocolo estándar PKCS#10 se puede utilizar sin adiciones entre el equipo del usuario y la red.

Una alternativa adicional permite que se indique alguna forma de cadena de nombre en el campo de asunto del mensaje PKS#10. Por ejemplo, en el caso de nombre usuario@campo, la parte del campo puede ser el identificador de servicio. En el caso de un nombre distinguido, la parte de la organización podría ser el identificador de servicio. Por ejemplo, nombre distinguido "CN=nombre de usuario, O=campo" podría usarse, como se describe en RFC 3280.

Como se ha mencionado anteriormente, la invención puede implementarse en arquitecturas distintas de la arquitectura del servidor http descrita anteriormente. En particular, las funciones de la puerta de enlace SEC (TLS) y el servidor http y las interfaces relacionadas (PK1, PK3, HT4, SP-AA) podría reemplazarse con una única función que recibe el certificado de suscriptor para la autentificación, opcionalmente valida el certificado (PK3), desafía al cliente y verifica la respuesta para autentificar al cliente (PK1), y proporciona el servicio solicitado a los clientes autorizados (HT4).

REIVINDICACIONES

1. Un método para autentificar un terminal de usuario que busca acceso a un servicio desde un proveedor de servicios en una red de comunicación, comprendiendo el método:

asignar al terminal de usuario una pluralidad de identidades específicas de servicio para acceder a servicios respectivos;
emitir una solicitud desde el terminal de usuario, identificando la solicitud el servicio al que se accede y que incluye una clave pública del terminal de usuario;
en una autoridad de certificación (10), autentificar la solicitud y emitir un certificado de clave pública para vincular una identidad específica del servicio con la clave pública en la solicitud y devolver el certificado de clave pública al terminal de usuario.

2. El método según la reivindicación 1, en el que la solicitud incluye un identificador de servicio que identifica el servicio al que se va a acceder y un identificador de solicitante que identifica el terminal de usuario, comprendiendo el método la etapa adicional de:
en la autoridad de certificación (10), correlacionar el identificador de servicio y el identificador solicitante con la identidad específica del servicio que se autentificará.

3. El método según la reivindicación 1, en el que la solicitud identifica la identidad específica del servicio y en donde el método comprende la etapa adicional de:
verificar por parte de la autoridad de certificación (10) que el terminal de usuario está autorizado para usar la identidad específica del servicio.

4. El método según la reivindicación 1, en el que la etapa de emisión comprende emitir la solicitud que comprende un mensaje que incluye una pluralidad de campos, conteniendo uno de dichos campos un identificador de servicio para identificar el servicio al que se accede.

5. El método según la reivindicación 4, en el que el campo que contiene el identificador de servicio es un campo sujeto.

6. El método según la reivindicación 4, en el que la etapa de emisión comprende emitir la solicitud que comprende un mensaje PKCS#10.

7. El método según la reivindicación 4, en el que la etapa de emisión comprende emitir la solicitud que comprende un mensaje CRMF.

8. El método según la reivindicación 4, en el que la etapa de emisión comprende emitir la solicitud que comprende un mensaje HTTP.

9. El método según la reivindicación 1, que comprende implementar las etapas de asignación, emisión, autentificación y devolución en una red de comunicaciones inalámbricas.

10. Un terminal de usuario para usar en una red de comunicaciones que comprende:

medios (50) para emitir una solicitud que identifica un servicio al que se debe acceder e incluye una clave pública;
medios (50) para recibir un certificado de clave pública emitido por una autoridad de certificación (10) que asocia una identidad específica del servicio para acceder al servicio con la clave pública; y
medios (50) para reenviar el certificado de clave pública a un proveedor de servicios para autentificar la identidad específica del servicio para el terminal de usuario y autorizar así el acceso al servicio.

11. El terminal de usuario según la reivindicación 10, que comprende además medios para establecer material clave compartido con la autoridad de certificación (10) antes de emitir la solicitud.

12. El terminal de usuario según la reivindicación 10, que comprende medios para generar un par de claves asimétricas que incluyen la clave pública y una clave privada.

13. El terminal de usuario según la reivindicación 10, que comprende medios para emitir dicha solicitud a través de una interfaz inalámbrica.

14. El terminal de usuario según la reivindicación 10, en el que la solicitud identifica el servicio utilizando al menos uno de: una cadena transparente; una dirección de campo, un identificador universal de recursos; un nombre distinguido.

15. El terminal de usuario según la reivindicación 10, en el que la identidad específica del servicio no está incluida en

la solicitud.

16. Un sistema de autentificación para su uso en una red de comunicaciones para permitir el acceso a un servicio desde un proveedor de servicios, comprendiendo el sistema:

una autoridad de certificación (10) que comprende medios para recibir una solicitud desde un terminal de usuario, identificando la solicitud el servicio al que se accede y que incluye una clave pública del terminal de usuario; y
en donde la autoridad de certificación (10) está dispuesta para autentificar la solicitud y emitir un certificado de clave pública para una identidad específica de servicio del servicio al que se accederá y devolver el certificado de clave pública al terminal de usuario.

17. El sistema de autentificación según la reivindicación 16, que comprende un servidor de autentificación (6) configurado para autentificar la identidad del terminal de usuario que emite la solicitud.

18. El sistema de autentificación según la reivindicación 16, en el que la autoridad de certificación (10) comprende una base de datos de federación (FD), estando configurada la base de datos de federación para asignar el servicio y los identificadores del solicitante a las identidades específicas del servicio para acceder a servicios respectivos.

19. El sistema de autentificación según la reivindicación 16, en el que dichos medios para recibir dicha solicitud comprenden medios para recibir dicha solicitud a través de una interfaz inalámbrica.

FIG. 1

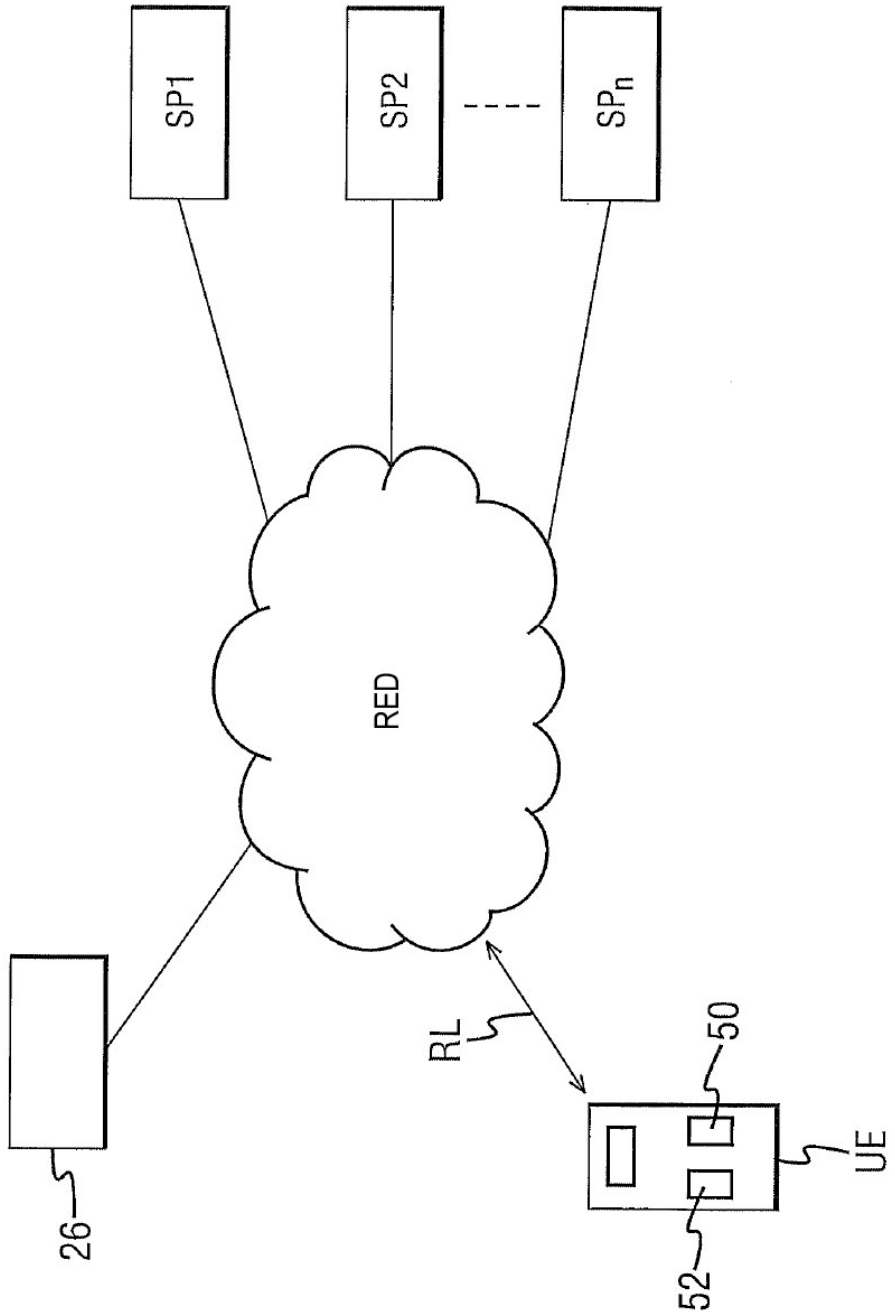


FIG. 2

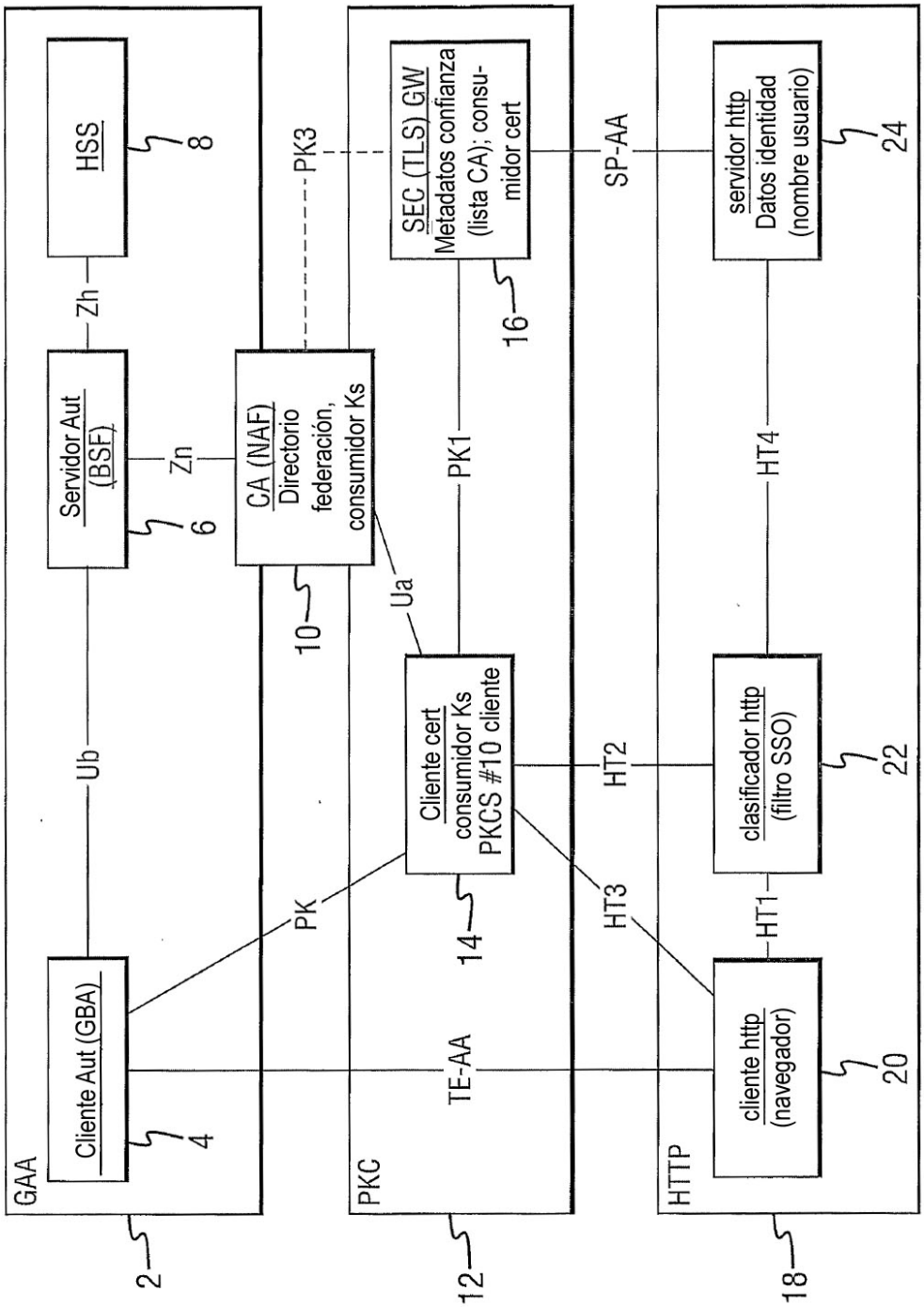

GAA
Cliente Aut (GBA)
4
Ub
Servidor Aut (BSF)
6
Zn
Zh
HSS
8
2
PKC
CA (NAF) Directorio federación, consumidor Ks
10
PK3
Ua
Cliente cert consumidor Ks PKCS #10 cliente
14
PK
PK1
SEC (TLS) GW Metadatos confianza (lista CA); consumidor cert
16
12
TE-AA
HTTP
cliente http (navegador)
20
HT1
HT2
HT3
clasificador http (filtro SSO)
22
HT4
servidor http Datos identidad (nombre usuario)
24
SP-AA
18

FIG. 3

FD

Nombre usuario	SI1	SSI1	K_s1
	SI_i	SSI_i	K_{si}
	SI_n	SSI_n	K_{sn}

FIG. 4

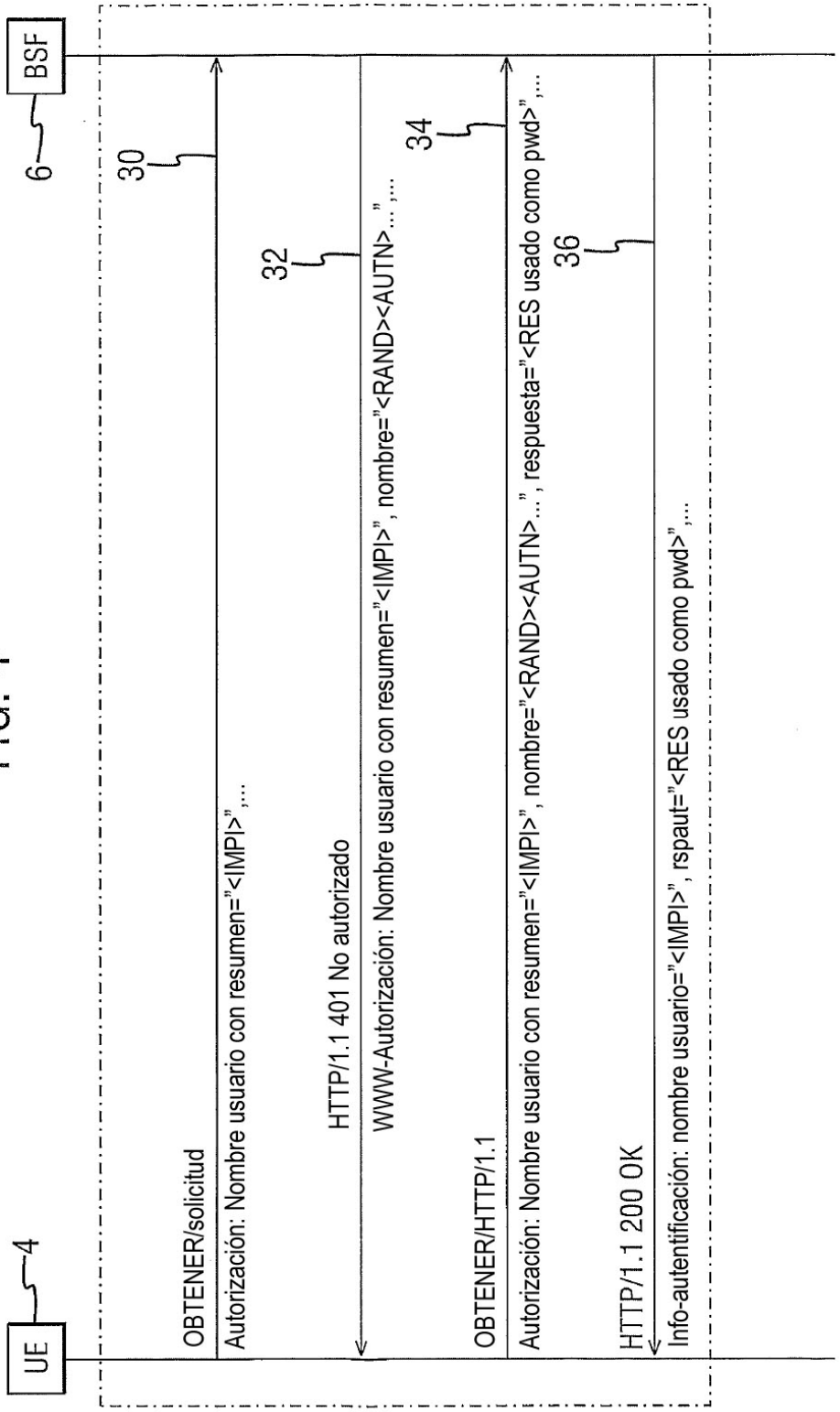
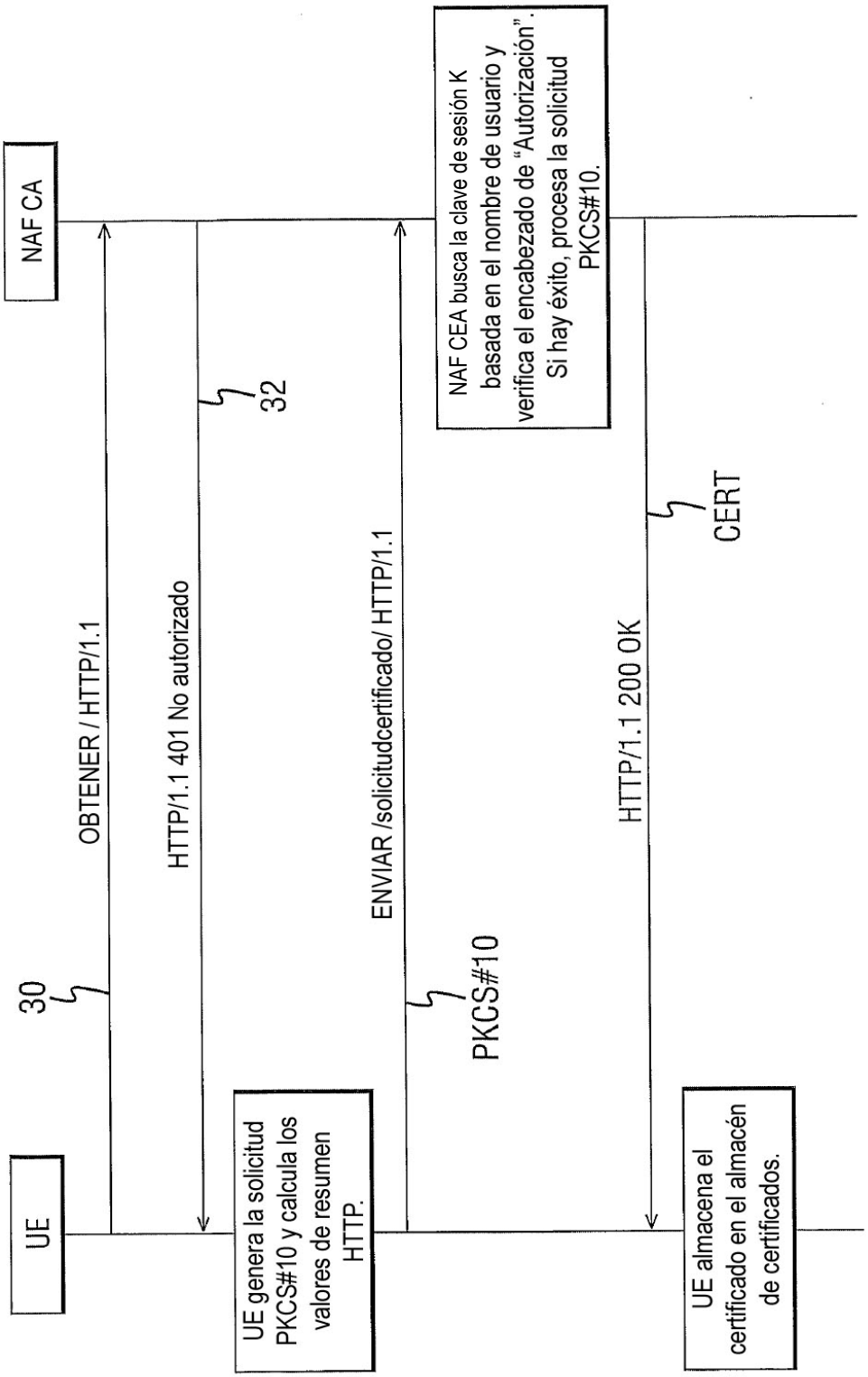

UE
4
BSF
6
30
OBTENER/solicitud
Autorización: Nombre usuario con resumen="<IMPI>",...
32
HTTP/1.1 401 No autorizado
WWW-Autorización: Nombre usuario con resumen="<IMPI>", nombre="<RAND><AUTN>...",...
34
OBTENER/HTTP/1.1
Autorización: Nombre usuario con resumen="<IMPI>", nombre="<RAND><AUTN>..." respuesta="<RES usado como pwd>",...
36
HTTP/1.1 200 OK
Info-autentificación: nombre usuario="<IMPI>", rspaut="<RES usado como pwd>",...

FIG. 5


UE
NAF CA
30
OBTENER / HTTP/1.1
HTTP/1.1 401 No autorizado
32
UE genera la solicitud PKCS#10 y calcula los valores de resumen HTTP.
ENVIAR /solicitudcertificado/ HTTP/1.1
PKCS#10
NAF CEA busca la clave de sesión K basada en el nombre de usuario y verifica el encabezado de "Autorización". Si hay éxito, procesa la solicitud PKCS#10.
HTTP/1.1 200 OK
CERT
UE almacena el certificado en el almacén de certificados.