(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 357 564**

(51) Int. Cl.:
H04W 12/06 (2006.01)
H04W 12/02 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03723560 .3**
(96) Fecha de presentación : **25.04.2003**
(97) Número de publicación de la solicitud: **1512307**
(97) Fecha de publicación de la solicitud: **09.03.2005**

(54) Título: **Método y sistema de autentificación de usuario en respuesta a instancia.**

(30) Prioridad: **12.06.2002 US 388503 P**
22.10.2002 US 278362

(45) Fecha de publicación de la mención BOPI:
27.04.2011

(45) Fecha de la publicación del folleto de la patente:
27.04.2011

(73) Titular/es: **Telefonaktiebolaget LM Ericsson (publ)**
Svardvagen 2
S-175 68 Järfälla, SE

(72) Inventor/es: **Blom, Rolf**

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

CAMPO TÉCNICO DE LA INVENCIÓN

La presente invención se refiere, generalmente, a procedimientos de autentificación en sistemas de comunicación y, más particularmente, a autentificación de usuario en respuesta a instancia, que implica una tercera parte intermediaria además del usuario y del centro de autentificación al que está asociado el usuario.

ANTECEDENTES DE LA INVENCIÓN

Muchos sistemas de comunicación actuales, incluyendo sistemas de comunicación móvil, sistemas de localización a distancia así como redes de datos sin hilos o inalámbricas y de líneas de cables, emplean procedimientos de autentificación y de encriptación o cifrado con el propósito de mejorar la seguridad y la robustez del sistema.

En los sistemas de comunicaciones móviles, por ejemplo, los usuarios se autentifican de cara a la red y/o a los proveedores de servicios con el fin de tener acceso a los servicios de la red, y la autentificación sirve también como base para la facturación a los usuarios. El protocolo de seguridad básico para los sistemas de comunicación por módem [modulador-desmodulador] implica normalmente un procedimiento de autentificación en respuesta a instancia, en la mayoría de los casos basado en criptografía de clave secreta. La autentificación en respuesta a instancia es bien conocida en la técnica y existen diversas normas sobre la autentificación básica en respuesta a instancia, por ejemplo, para redes de GSM (Sistema Global para Comunicaciones Móviles –"Global System for Mobile Communications") y de UMTS (Sistema de Telecomunicaciones Móviles Universal –"Universal Mobile Telecommunications System").

Tal como se ilustra en la Figura 1, un escenario típico en un sistema de comunicación por módem no solo implica al usuario y el centro de autentificación al que está asociado el usuario, sino también a una parte intermedia o intermediaria, tal como un operador de red independiente u otro proveedor de servicios. Típicamente, el centro de autentificación está relacionado con un operador doméstico con el que el usuario tiene una relación de confianza, por ejemplo, establecida a través de una suscripción o de una cuenta de prepago. Esta relación de confianza establecida se plasma, típicamente, en una relación criptográfica, por ejemplo, a través de una clave secreta compartida (criptografía simétrica). El centro de autentificación de operador doméstico, o, más específicamente, el operador de red doméstica, puede tener un acuerdo de servicio con la parte intermediaria, acuerdo que se plasma o materializa, típicamente, por una relación criptográfica similar. Sin embargo, la relación entre el usuario y el intermediario se considera, por lo común, como una relación de confianza inducida que se establece cuando los servicios ofrecidos por la parte intermediaria son solicitados o de otra forma iniciados.

La Figura 2 es un diagrama esquemático de un procedimiento de autentificación en respuesta a instancia típico de la técnica anterior, que implica a un usuario, un centro de autentificación de operador doméstico asociado y una parte intermediaria. Por ejemplo, el procedimiento de AKA (Acuerdo sobre Autentificación y Clave –"Authentication and Key Agreement") convencional que se utiliza en sistemas de comunicaciones tales como las redes de GSM y de UMTS, incluye un procedimiento de respuesta ante instancia basado en una clave secreta. La clave secreta, denotada por K_i, es por lo común la clave de suscripción asociada con una suscripción o abono de usuario-operador, o una clave obtenida de la misma. El intermediario puede ser, por ejemplo, un nodo de red que gestiona una red dentro de la que se está trasladando el usuario en desplazamiento itinerante, u otro tipo de proveedor de servicios que ofrece servicios en relación con el usuario.

Para la autentificación de un usuario dado en la parte intermediaria, se le solicita normalmente al usuario enviar una ID de usuario a la parte intermediaria, la cual, a su vez, remite esta ID al centro de autentificación de operador doméstico en una solicitud de datos de autentificación. Con el fin de ayudar a la autentificación del usuario, el centro de autentificación doméstico genera una respuesta esperada XRES ("expected response") basándose en la clave secreta K_i asociada con este usuario particular y en una instancia aleatoria RAND ("random") como entradas para una función *g* dada. Normalmente, el centro de autentificación puede generar también información adicional tal como una clave de confidencialidad, una clave de integridad y una ficha de autentificación. En el AKA de GMS, no se utiliza ninguna clave de integridad ni ficha de autentificación, pero el procedimiento básico de respuesta ante instancia es el mismo. La RAND de instancia y la respuesta esperada XRES, conjuntamente con la información adicional, son enviadas a la parte intermediaria que desea autentificar al usuario. La parte intermediaria remite la RAND de instancia y, posiblemente, la ficha de autentificación al usuario. El usuario, preferiblemente con la ayuda de un módulo de identidad de abonado (SIM –"subscriber identity module"– o USIM), genera una respuesta RES basándose en la clave secreta compartida K_i (almacenada de forma segura en al SIM o el USIM), y la RAND de instancia recibida, como entradas para la misma función *g* que se utiliza por el centro de autentificación. El usuario envía entonces la respuesta RES recibida de vuelta a la parte intermediaria. Para autentificar al usuario, la parte intermediaria simplemente verifica que la respuesta RES recibida del usuario es igual a la respuesta XRES esperada recibida del centro de autentificación.

La transmisión de parámetros de autentificación entre el centro de autentificación y la parte intermediaria puede ser protegida criptográficamente. En el UMTS, por ejemplo, puede utilizarse el protocolo de seguridad MAPSec. El protocolo MAPSec ha sido normalizado en 3GPP [Proyecto de Sociedad de 3ª Generación –"3rd Generation Partnership Project"], pero no se ha desarrollado.

Se requiere normalmente que sea posible distribuir con antelación los datos de autentificación y que

sea posible llevara a cabo el procedimiento de autentificación ulteriormente, sin un contacto renovado con el centro de autentificación.

Existen dos amenazas principales para el anterior procedimiento básico de autentificación en respuesta a instancia. El primer peligro es que una tercera parte malintencionada, tal como un operador de red independiente u otro proveedor de servicios, pueda solicitar datos de autentificación del centro de autentificación y, con posterioridad, afirmar falsamente que un usuario ha estado trasladándose de forma itinerante dentro de la red o ha utilizado de otro modo servicios ofrecidos, y finalmente requerir el pago de los servicios. El centro de autentificación no puede pedir ninguna prueba que lo corrobore, ya que los sistemas actuales no tienen capacidad para semejante función.

El segundo peligro es que puedan interceptarse parámetros de autentificación cuando son enviados desde el centro de autentificación a la parte intermediaria, o leídos en un nodo ilícitamente intervenido o «pirateado» de la parte intermediaria. Los parámetros de autentificación sustraídos pueden ser entonces utilizados para autentificarse de forma fraudulenta como el usuario al que están asociados los parámetros. Semejante ataque se basa en la habilidad para robar los datos de autentificación y utilizarlos antes de que lo haga el usuario verdadero. Por ejemplo, dicho ataque es posible cuando un usuario se está desplazando de forma itinerante entre redes y los parámetros de autentificación se almacenan para un uso ulterior en la red de la que está saliendo el usuario.

TÉCNICA RELACIONADA

En la Patente norteamericana Nº 5.596.641 se describe un método de autentificación de una unidad móvil de desplazamiento itinerante en sistemas de comunicación móvil. El método comprende dos etapas: una etapa de autentificación preliminar y una etapa de autentificación principal. En la etapa preliminar, una pluralidad de pares de primeras instancias y respuestas esperadas son enviados desde una red doméstica a una red en la que se está realizando un desplazamiento itinerante. Terceras instancias formadas por el acoplamiento de segundas instancias y las primeras instancias, son transmitidas a la unidad móvil en desplazamiento itinerante, la cual calcula y transmite respuestas a la red en la que se está realizando el desplazamiento itinerante. En la etapa de autentificación principal, las unidades móviles son entonces autentificadas utilizando un par de segundas instancias y respuestas calculadas.

En la Patente norteamericana Nº 5.537.474 y en la Patente norteamericana Nº 5.668.875 se describen un método y un aparato para autentificar un abonado en desplazamiento itinerante en un sistema de comunicación. Un abonado y su sistema doméstico asociado utilizan instancias y respuestas de un protocolo de autentificación de sistema doméstico, y un sistema en el que se realiza el desplazamiento itinerante utiliza un protocolo de autentificación local correspondiente. El abonado convierte cualquier instancia recibida desde el sistema en que se realiza el desplazamiento itinerante en un formato compatible con el protocolo de sistema doméstico. Una respuesta de usuario generada se convierte al protocolo de autentificación local antes de ser transmitida al sistema en el que se está realizando el desplazamiento itinerante. La instancia y la respuesta de usuario son entonces remitidas desde el sistema en que se realiza el desplazamiento itinerante al sistema doméstico, en el que se lleva a cabo una conversión similar antes de autentificar al abonado basándose en la respuesta de usuario y en la respuesta esperada.

La Patente norteamericana Nº 5.991.407 describe un procedimiento de autentificación en un sistema de comunicaciones móviles basado en GSM, que utiliza un algoritmo A3 para calcular una respuesta firmada a partir de una instancia y una clave de autentificación dentro de una unidad móvil. Se emplea un algoritmo de CAVE (Autentificación y Cifrado de Voz Celulares –“Cellular Authentication and Voice Encryption”) como algoritmo A3. Se proporcionan funciones de adaptación de parámetros entre la entrada del algoritmo de CAVE y la entrada de instancia y clave de autentificación, así como entre la salida del algoritmo de CAVE y la salida de respuesta firmada.

La Patente norteamericana Nº 6.389.536 B1 divulga un dispositivo que verifica calificaciones para el uso de programación o software distribuido desde un proveedor de contenidos a un aparato de usuario. Para poder llevar a cabo o ejecutar el software obtenido, el aparato de usuario se autentifica, en primer lugar, por medio de tres instrumentos de inclusión en el dispositivo de verificación. Un instrumento de emisión de información de soporte de prueba, dispuesto en el proveedor de contenidos, emite información de soporte de prueba, por ejemplo, en forma de un tique enviado a un instrumento de probatura ubicado en el aparato de usuario, al solicitarse una ejecución de software. El instrumento de probatura genera información de respuesta basándose en la información de soporte de prueba, conjuntamente con una instancia obtenida de un instrumento de verificación embebido o incluido en el software. Esta información de respuesta es transmitida al instrumento de verificación y utilizada para propósitos de autentificación. Si se ha autentificado correctamente, el instrumento de verificación permite al aparato de usuario ejecutar el software.

Las Patentes anteriormente indicadas se ven afectadas por los mismos o similares problemas que el procedimiento de respuesta ante instancia de la técnica anterior que se ha expuesto con referencia a la Figura 2.

El documento WO-A-01 76134 se refiere a un método para la autentificación mutua de un nodo móvil y una red de datos en paquetes, que comprende un procedimiento de respuesta ante instancia que involucra un nodo móvil y una red de datos en paquetes. El nodo móvil y la red de datos en paquetes comparten un secreto. El nodo móvil está provisto de un código de protección y envía una identidad de nodo móvil y el código de protección a la red. La red genera un secreto de sesión correspondiente a la identidad, a partir del secreto compartido y de una instancia. La red

conforma una información criptográfica utilizando al menos el código de protección y el secreto de sesión. La red envía al nodo móvil la instancia y la información criptográfica, gracias a lo cual el nodo móvil puede verificar la información criptográfica utilizando la instancia y el secreto compartido, generar el secreto de sesión y generar una respuesta correspondiente a la instancia, basándose en el secreto compartido. La respuesta generada es enviada a la red para la autentificación del nodo móvil.

En el documento US-A-5.491.750 se divulga un método para identificar partes en comunicación en virtud del cual un intermediario actúa deduciendo de claves secretas de larga duración, proporcionadas por adelantado a la parte intermediaria y a una parte concreta en comunicación, una clave de corta vida. Tras ello, la parte intermediaria, al recibir una petición de comunicación entre los partícipes en la comunicación, actúa distribuyendo la clave de corta vida a los partícipes en la comunicación, por lo que la distribución se ve protegida por el enmascaramiento de la clave de corta vida utilizando la clave de larga duración de la parte respectiva en comunicación. La parte intermediaria, por otro lado, lleva a cabo la autentificación de las partes en comunicación y, al depositarse en ella la confianza de cada parte en comunicación, permite, con ello, que las partes en comunicación se induzcan confianza mutuamente.

Una propiedad característica del método comprende el hecho de que el intermediario cuenta con la confianza de las partes en comunicación y está provisto de claves secretas de larga duración compartidas con los partícipes correspondientes.

En el documento US-A-6.058.480 se divulga un sistema y un método para la autentificación de usuarios y servicios en comunicación a través de una red no segura. Cada uno de un usuario y un servicio tiene una frase de paso que se mantiene en secreto a lo largo de todo el procedimiento de autentificación basado en respuesta ante instancia. Una entidad de autentificación proporciona soporte a la autentificación al recibir datos de autentificación procedentes de un servicio para su verificación, los cuales incluyen datos de autentificación de usuario recibidos desde un usuario en comunicación. El ente de autentificación conoce la frase de paso de los usuarios y servicios, lo que hace posible la verificación de datos de respuesta obtenidos de la respectiva frase de paso. Más específicamente, las partes de autentificación intercambian instancias aleatorias para la generación de la respectiva respuesta. El usuario envía la respuesta al servicio, que remite su propia respuesta y la respuesta del usuario al ente de autentificación.

SUMARIO DE LA INVENCIÓN

La presente invención supera estas y otras desventajas de las disposiciones de la técnica anterior.

Es un propósito general de la presente invención proporcionar un procedimiento de autentificación de respuesta ante instancia mejorado. En particular, es deseable proporcionar un procedimiento de autentificación que permita a una parte intermedia o intermediaria presentar una evidencia válida de que un usuario ha sido realmente autentificado. Esto evitaría de un modo eficaz que proveedores de servicios malintencionados afirmen falsamente que los usuarios han aceptado y hecho uso de sus servicios, y también impide la no repudiación de la autentificación por parte de los usuarios. Puede también ser importante evitar y/o desbaratar ataques de intercepción.

Es un propósito de la invención proporcionar un método y un sistema mejorados para autentificar a un usuario y una parte intermedia basándose en un procedimiento de respuesta ante instancia de clave secreta (criptografía simétrica).

Es también un propósito de la invención proporcionar un centro de autentificación mejorado para ayudar a la autentificación de un usuario y una parte intermediaria asociados.

Aún otro propósito de la invención consiste en proporcionar un nodo de red de parte intermediaria gestionado por el proveedor de servicios para la autentificación de un usuario asociado con un centro de autentificación.

Estos y otros propósitos se consiguen por medio de la invención según se define por las reivindicaciones de Patente que se acompañan.

A fin de mejorar el procedimiento básico de autentificación en respuesta a instancia de clave secreta (criptografía simétrica), una idea básica es enmascarar la respuesta esperada generada por el centro de autentificación, por medio de una función de enmascaramiento, y transmitir la respuesta esperada enmascarada, en lugar de la respuesta esperada propiamente dicha, a una parte intermediaria en la que tiene lugar la autentificación real. La parte intermediaria recibe una respuesta de usuario del usuario correspondiente y también genera una respuesta de usuario enmascarada utilizando la misma función de enmascaramiento que el centro de autentificación. A fin de autentificar al usuario, la parte intermediaria verifica entonces que la respuesta de usuario enmascarada corresponde a la respuesta esperada enmascarada que se ha recibido desde el centro de autentificación.

El anterior procedimiento de respuesta ante instancia hace posible que la parte intermediaria demuestre que el usuario se ha autentificado adecuadamente, y, al mismo tiempo, impide y/o desbarata los ataques de intercepción como consecuencia del enmascaramiento de la respuesta esperada.

La idea que subyace en la solución propuesta es que un atacante, tal como un usuario autorizado que

intercepta parámetros de autentificación o una parte intermediaria malintencionada, no debe conocer la respuesta de antemano. Son únicamente el usuario legítimo y el centro de autentificación quienes conocen inicialmente la respuesta y la respuesta esperada, respectivamente. De acuerdo con ello, la idea es impedir que tanto los atacantes de intercepción como la parte intermediaria consigan acceder a la respuesta esperada, pero permitir, con todo, que la parte intermediaria autentifique al usuario basándose en la respuesta del usuario subsiguientemente transmitida desde el usuario. Como se ha explicado anteriormente, esto puede lograrse enmascarando la respuesta esperada en el centro de autentificación antes de transmitirla a la parte intermediaria, y generando una respuesta de usuario enmascarada correspondiente en la parte intermediara con el fin de permitir la autentificación. Con este procedimiento, la parte intermediaria puede ahora utilizar la respuesta recibida desde el usuario así como la información de identificación de usuario correspondiente, preferiblemente junto con la instancia asociada que se ha utilizado para generar la respuesta, para demostrar que este usuario particular ha sido realmente autentificado. En consecuencia, partes intermediarias, por ejemplo, proveedores de servicios, pueden ser instadas a proporcionar valores de respuesta o pares respuesta-instancia con el fin de demostrar que usuarios han estado realmente presentes en la red y/o utilizado otros servicios, antes de que se transfieran los pagos.

Como ya se ha mencionado anteriormente, un atacante que intercepte los parámetros de autentificación entre el centro de autentificación y la parte intermediaria puede, obviamente, no utilizar estos parámetros directamente para hacerse pasar por un usuario legítimo.

La prueba de la autentificación de un usuario puede gestionarse en un procedimiento fuera de conexión o bajo conexión, o en línea. En el primer caso, se almacena información de prueba de autentificación, que incluye al menos la respuesta del usuario recibida del usuario y, preferiblemente, también la instancia correspondiente, en una ubicación de almacenamiento desde la cual puede ser recuperada ulteriormente por la parte intermediaria y presentada como evidencia de la autentificación del usuario. En el último caso, la información de prueba de autentificación es remitida más o menos directamente desde la parte intermediaria al centro de autentificación, lo que hace posible una prueba bajo conexión o en línea. Basándose en la información de prueba de autentificación presentada, el centro de autentificación puede entonces llevar a cabo un(os) cálculo(s) y/o comparación (comparaciones) relevante(s) con el fin de verificar si la parte intermediaria ha autentificado realmente a un usuario dado.

La función de enmascaramiento pude ser una función privada solo conocida por el centro de autentificación y por la parte intermediaria, o bien una función públicamente conocida, y tiene, generalmente, propiedades en un solo sentido, o no invertibles, y/o distributivas. Para una seguridad incrementada, especialmente para refrenar o detener ataques previos a la computación, el cálculo de la respuesta esperada enmascarada y el cálculo de la respuesta de usuario enmascarada pueden llevarse a cabo basándose en una instancia aleatoria de enmascaramiento común, denotada como SALT. La instancia aleatoria de enmascaramiento común, SALT, puede ser completamente aleatoria, independiente de la instancia aleatoria, denotada como RAND [“random challenge”], que se utiliza para generar la respuesta de usuario / respuesta esperada, y, por tanto, ser transmitida conjuntamente con la RAND a la parte intermediaria.

Sin embargo, con el fin de evitar un intercambio de señales adicional entre las entidades implicadas, la instancia aleatoria de enmascaramiento SALT puede ser deducida de instancia aleatoria RAND. En este caso, la instancia aleatoria RAND es transmitida, como es habitual, a la parte intermediaria y remitida al usuario. Puede calcularse entonces la instancia aleatoria de enmascaramiento SALT a partir de la RAND transmitida en la parte intermediaria, y utilizarse subsiguientemente para generar la respuesta de usuario enmascarada. Una solución efectiva a este respecto consiste en reutilizar sencillamente la instancia aleatoria RAND como instancia aleatoria de enmascaramiento SALT.

Con el fin de permitir una suave migración en relación con las infraestructuras existentes, se recomienda que se notifique a la parte intermediaria sobre si se ha utilizado o no la función de enmascaramiento a la hora de calcular la respuesta esperada distribuida. De esta forma, el protocolo para distribuir parámetros de autentificación se extiende o prolonga, preferiblemente, con tal indicación.

Una amenaza adicional es que una parte intermediaria malintencionada pueda enviar la información de prueba a otra parte que, a su vez, presente la información de prueba al centro de autentificación en una petición de pago (presumiblemente, de servicios más caros). Además, puede ser también posible que un atacante lea la información de prueba en un nodo del proveedor de servicios ilícitamente intervenido o «pirateado», y utilice la información para solicitar el pago de servicios. Este problema particular puede ser resuelto mediante la asociación de datos de datos de autentificación generados por el centro de autentificación para un usuario dado, a la parte intermediaria que participa en la autentificación del usuario, al objeto de vincular información de prueba correspondiente a la parte intermediaria. Preferiblemente, los datos de autentificación están interrelacionados, en el centro de autentificación, con una indicación de la parte intermediaria, y los datos de autentificación son subsiguientemente comparados, en el centro de autentificación, con información de prueba recibida (o una representación de la misma), a fin de verificar que la información de prueba está asociada con la parte intermediaria.

La invención ha resultado ser particularmente útil en sistemas de comunicación móviles, tales como las redes de GSM o de UMTS, si bien no están limitados por estas.

La invención, que, en su conjunto, constituye una solución ciertamente elegante, ofrece las siguientes ventajas:

- Permitir que las partes intermediarias, tales como proveedores de servicios, demuestren que los usuarios han sido realmente autentificados;

- Impedir que proveedores de servicios malintencionados afirmen falsamente que los usuarios han aceptado sus servicios;

- Impedir la no repudiación de la autentificación de usuario por parte de los usuarios;

- Desbaratar de forma efectiva los ataques de intercepción, ya que la(s) función (funciones) de enmascaramiento hace(n) prácticamente imposible sustraer los datos reales de autentificación;

- Posibilidad de vincular información de prueba con una parte intermediaria dada; y

- Proporcionar una fácil migración con infraestructura ya existente.

Otras ventajas ofrecidas por la presente invención se apreciarán por la lectura de la descripción que sigue de realizaciones de la invención.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La invención, conjuntamente con objetos y ventajas adicionales de la misma, se comprenderá mejor con referencia a la descripción que sigue, tomada en combinación con los dibujos que se acompañan, en los cuales:

la Figura 1 es una global o de conjunto de un sistema de comunicaciones que ilustra las partes relevantes del procedimiento de autentificación y sus relaciones mutuas;

la Figura 2 es un diagrama esquemático de un procedimiento de autentificación en respuesta a instancia típico de la técnica anterior, que ilustra la transmisión de información entre las partes relevantes;

la Figura 3 es un diagrama de flujo de un procedimiento general de autentificación en respuesta a instancia de acuerdo con la invención;

la Figura 4 es un diagrama esquemático de un ejemplo de procedimiento de autentificación en respuesta a instancia de acuerdo con la invención, que ilustra la transmisión de información entre las partes relevantes;

la Figura 5A es un diagrama de flujo que ilustra con mayor detalle la etapa de generación y enmascaramiento de respuesta esperada de la Figura 3;

la Figura 5B es un diagrama de flujo que ilustra con mayor detalle la etapa de transmisión de respuesta esperada enmascarada de la Figura 3;

la Figura 5C es un diagrama de flujo que ilustra con mayor detalle la etapa de generación y transmisión de respuesta de usuario de la Figura 3;

la Figura 5D es un diagrama de flujo que ilustra con mayor detalle la etapa de generación de respuesta de usuario enmascarada de la Figura 3;

la Figura 5E es un diagrama de flujo que ilustra con mayor detalle la etapa de verificación de la Figura 3;

la Figura 6 es un diagrama de bloques esquemático de un ejemplo de un centro de autentificación de acuerdo con una realización preferida de la invención;

la Figura 7 es un diagrama de bloques esquemático de un ejemplo de una parte intermediaria de acuerdo con una realización preferida de la invención;

la Figura 8 es un diagrama de bloques esquemático de una realización proporcionada a modo de ejemplo de un sistema de autentificación ilustrado como un sistema de red doméstico con una unidad móvil asociada que se desplaza de forma itinerante dentro de un sistema de red visitado;

la Figura 9 es un diagrama de bloques esquemático de otra realización proporcionada a modo de ejemplo de un sistema de red doméstico de acuerdo con la invención, con el algoritmo de autentificación doméstico y el HLR (Registro de Posiciones Domésticas –“Home Location Register”) implementados en diferentes nodos de red;

la Figura 10 es un diagrama de bloques esquemático de aún otra realización proporcionada a modo de ejemplo de un sistema de red doméstico de acuerdo con la invención, con el algoritmo de autentificación doméstico distribuido entre varios nodos de red; y

la Figura 11 es un diagrama esquemático que ilustra un corredor que actúa como un centro de autentificación para un cierto número de operadores de red diferentes.

DESCRIPCIÓN DETALLADA DE REALIZACIONES DE LA INVENCIÓN

Se utilizarán a lo largo de los dibujos los mismos caracteres de referencia para elementos correspondientes o similares.

Con el fin de llegar a una comprensión básica e intuitiva de la invención, se comenzará por describir un procedimiento básico de autentificación en respuesta a instancia con referencia a la Figura 3. Se supone aquí que las partes implicadas incluyen un usuario, un centro de autentificación al que está asociado el usuario, y una parte intermedia o intermediaria que desea autentificar al usuario. En este ejemplo, se supone, además, que la autentificación global está basada en un procedimiento de respuesta ante instancia en el que el centro de autentificación genera una respuesta esperada y el usuario genera, subsiguientemente, una respuesta correspondiente. Una idea básica es introducir una función de enmascaramiento, la cual enmascara la respuesta esperada generada (S1). La respuesta generada enmascarada es entonces transmitida a la parte intermediaria (S2). El usuario genera y transmite una respuesta de usuario correspondiente de una manera convencional (S3). La parte intermediaria recibe, de esta forma, una respuesta esperada enmascarada desde el centro de autentificación, así como la respuesta de usuario habitual por parte del usuario. La parte intermediaria genera entonces una respuesta de usuario enmascarada por medio de la misma función de enmascaramiento (S4) y, por último, compara la respuesta esperada enmascarada y la respuesta de usuario enmascarada con el fin de verificar la autentificación del usuario (S5). De esta forma, la parte intermediaria es capaz de demostrar que el usuario ha sido autentificado, teniendo en mente que es únicamente el usuario / centro de autentificación legítimo el que inicialmente conoce la respuesta / respuesta esperada. Un proveedor de servicios malintencionado o un usuario no autorizado no puede conocer la respuesta de antemano. De acuerdo con ello, al enmascarar la respuesta esperada en el centro de autentificación antes de transmitirla a la parte intermediaria, la parte intermediaria así como los atacantes de intercepción se ven impedidos de obtener el acceso a la respuesta esperada no enmascarada. La generación de una respuesta de usuario enmascarada correspondiente, sin embargo, sigue permitiendo que la parte intermediaria autentifique al usuario. Esto significa que la parte intermediaria puede utilizar la respuesta recibida desde el usuario, de preferencia conjuntamente con la instancia asociada utilizada para generar la respuesta, para demostrar que este usuario particular ha sido realmente autentificado. En consecuencia, partes intermediarias, por ejemplo, proveedores de servicios, pueden ser instadas a proporcionar valores de respuesta o, preferiblemente, pares respuesta-instancia con el fin de demostrar que los usuarios han estado realmente presentes en la red y/o han utilizado otros servicios, antes de que se transfieran los pagos.

Aparentemente, el centro de autentificación y la parte intermediaria tienen una relación que implica que se ha intercambiado la función de enmascaramiento entre el centro de autentificación y la parte intermediaria. Esto también es cierto para información similar y/o funciones que tienen que ser comunes para las dos partes.

Debe comprenderse que la expresión “centro de autentificación” es una expresión genérica, no limitada al nodo de Centro de Autentificación (AuC –“Authentication Center”) que se encuentra habitualmente en los sistemas de comunicación móvil por módem. El centro de autentificación de acuerdo con la invención puede, de hecho, ser cualquier centro que gestione o participe de otra manera en la autentificación de un usuario del modo aquí descrito. Por ejemplo, el centro de autentificación puede ser, naturalmente, un centro de autentificación de operador doméstico, que implique, posiblemente, un servidor de AAA (Autorización, Autentificación y Contabilidad –“Authorization, Authentication and Accounting”) que puede o no estar ubicado conjuntamente con el centro de autentificación. Sin embargo, puede ser también un corredor que actúe como un centro de autentificación general, o centro de identidad, para un cierto número de operadores de red o proveedores de servicios diferentes.

La parte intermediaria puede ser cualquier parte intermediaria en la que se haya autentificado el usuario de acuerdo con la presente invención, incluyendo un nodo de red que gestiona una red “visitada” dentro de la cual se está desplazando de forma itinerante el usuario, un proveedor de servicios de web, un proveedor de contenidos y, de hecho, incluso el propio MSC / VLR (Centro de Conmutación Móvil / Registro de Posiciones Visitadas –“Mobile Switching Center” / “Visited Location Register”) del operador doméstico.

En el caso de una red visitada en la que se está desplazando de forma itinerante un usuario, el operador de la red visitada puede también ofrecer otros servicios, tales como servicios de web o incluso contenidos digitales, además de los servicios básicos de acceso a red. Sin embargo, si el proveedor de servicios de web y/o el proveedor de contenidos son independientes del operador de la red visitada, la situación se vuelve algo más compleja. El operador de la red visitada puede, por supuesto, tener alguna relación con los otros proveedores de servicios, los cuales pueden pedir al operador confirmación de que un usuario dado ya ha sido autentificado por el operador. Alternativamente, sin embargo, el procedimiento de autentificación en respuesta a instancia propuesto por la invención se repite para cada parte intermediaria independiente, tal como un proveedor de acceso a red, un proveedor de servicios de web y un proveedor de contenidos. En este último caso, cada proveedor de servicios obtendrá entonces su propia información de prueba de autentificación.

El MSC / VLR del propio operador doméstico puede también actuar como una parte intermediaria que interactúa con el centro de autentificación, tal como el centro de autentificación de operador doméstico o un centro de

identidad general, en la autentificación de usuarios que desean acceder a la red. Si el MSC / VLR y el centro de autentificación son gestionados por el mismo operador doméstico, no es, generalmente, necesario que el MSC / VLR almacene información de prueba de autentificación. En lugar de ello, el propósito principal del enmascaramiento es proteger la respuesta esperada transmitida entre el centro de autentificación y el nodo de MSC / VLR contra ataques de intercepción. Por otra parte, si el centro de autentificación es un centro de identificación general que actúa como un corredor del centro de autentificación para el operador doméstico del usuario, es ciertamente interesante que el MSC / VLR del operador doméstico almacene información de prueba de autentificación de usuario, la cual puede utilizarse ulteriormente para demostrar que un usuario dado ha sido realmente autentificado en el MSC / VLR. Puede ser también conveniente disponer de un procedimiento de autentificación normalizado que sea el mismo con independencia de si la parte intermediaria es gestionada por el operador doméstico o por un tercero o parte externa. En el caso de servicios diferentes de los servicios básicos de acceso a red, el intercambio de señales requerido se produce generalmente en el nivel de aplicación de la pila de protocolos. En este caso, es, típicamente, una aplicación ubicada en el terminal de usuario la que inicia el procedimiento de autentificación (y de acuerdo sobre clave). Puede encontrarse información general sobre los mecanismos para permitir que las aplicaciones del terminal inicien el AKA, en la divulgación de H. Haverinen: "*EAP SIM Authentication*" ("Autentificación de SIM de EAP"), Internet Draft of the Internet Engineering Task Force [Borrador en Internet del Grupo de Trabajo de Ingeniería de Internet].

Como ya se ha mencionado, la parte intermediaria puede ser también un proveedor de servicios de web, o bien un proveedor de contenidos que distribuye datos en medios de soporte de información digitales tales como audio, vídeo, imágenes, libros electrónicos y software o programación a un usuario. En el caso del proveedor de contenidos, la autentificación de acuerdo con la invención se lleva a cabo, preferiblemente, antes de la descarga o generación de corrientes de datos real de medios de soporte de información al usuario.

En realidad, cualquier parte que proporcione servicios tales como servicios de acceso a red, servicios de web, servicios de contenidos o servicios de correduría de pagos, puede actuar como parte intermediaria según se utiliza en la presente descripción.

Para una mejor comprensión de la invención, se describirá a continuación un ejemplo más completo de un ejemplo de autentificación de acuerdo con la presente invención, con referencia a la Figura 4, la cual ilustra la transmisión de información de autentificación entre las partes relevantes, así como a los diagramas de flujo de las Figuras 5A-E.

En general, la autentificación global es iniciada por un usuario al transmitir una ID de usuario a una parte intermediaria, la cual, a su vez, remite la ID de usuario a un centro de autentificación asociado, a modo de petición de datos de autentificación. Basándose en la ID de usuario recibida, el centro de autentificación identifica una clave secreta simétrica / compartida K_i asociada con el usuario particular. Por ejemplo, la clave K_i puede ser una clave de suscripción o abono, en el caso de que el usuario tenga una suscripción con un operador doméstico, o una clave criptográfica asociada con una cuenta de prepago. El centro de autentificación genera una instancia aleatoria RAND ("random challenge") (S11) y calcula una respuesta esperada XRES ("expected response") (S12) basándose en la clave secreta K_i y en la instancia aleatoria RAND, como entradas para una función dada *g*. El centro de autentificación genera entonces, preferiblemente, una instancia aleatoria de enmascaramiento SALT (S13), por ejemplo, como un valor aleatorio completamente independiente o basado en la instancia aleatoria RAND, y utiliza esta instancia aleatoria de enmascaramiento SALT y la respuesta esperada calculada XRES como entradas para una función de enmascaramiento *f*, a fin de calcular una respuesta esperada enmascarada XRES' (S14). Subsiguientemente, la respuesta esperada enmascarada XRES' y la instancia aleatoria RAND son transmitidas (S21), posiblemente junto con la SALT aleatoria de enmascaramiento opcional (S22), a la parte intermediaria.

Para una parte intermediaria que es completamente externa al centro de autentificación o independiente de este, se requiere también, por lo común, que la parte intermediaria reciba información del usuario que pueda ser utilizada para determinar la identidad del centro de autentificación al que está asociado el usuario y, más concretamente, la identidad del operador doméstico del usuario. Esto permite que la parte intermediaria envíe la petición de datos de autentificación al centro de autentificación / operador doméstico relevante, teniendo en mente que el centro de autentificación puede ser el centro de autentificación de un operador doméstico particular o un corredor que actúa como un centro de autentificación general o centro de identidad. En este último caso, se requiere normalmente la identidad del operador doméstico para encontrar información de clave secreta relevante, tal y como se explicará más adelante con referencia a la Figura 11.

Una vez recibida, la parte intermediaria remite la instancia aleatoria RAND al usuario (S31). El usuario calcula entonces una respuesta RES de usuario (S32) con la instancia aleatoria RAN y la copia del usuario de la clave secreta compartida K_i, como entradas a la misma función *g* que ha utilizado el centro de autentificación para calcular la respuesta esperada XRES. La respuesta RES de usuario obtenida se transmite a la parte intermediaria (S33) para su uso en la autentificación subsiguiente.

Si la instancia aleatoria de enmascaramiento opcional SALT no fue explícitamente transmitida desde el centro de autentificación, la parte intermediaria puede deducirla (S41) antes de la verificación de la autentificación, basándose, preferiblemente, en la instancia aleatoria RAND. Se calcula una respuesta de usuario enmascarada RES' por la parte intermediaria (S42), por medio de la respuesta RES de usuario y la instancia aleatoria de enmascaramiento

opcional, recibida o deducida, SALT, como entradas para la función de enmascaramiento *f*. Tras ello, la parte intermediaria compara (S51) la respuesta de usuario enmascarada calculada RES' con la respuesta esperada enmascarada XRES' obtenida desde el centro de identificación. Si la respuesta de usuario enmascarada RES' corresponde a la respuesta esperada enmascarada XRES', la parte intermediaria ha autentificado al usuario (S52).

Tal y como se ha mencionado brevemente en lo anterior, la instancia aleatoria de enmascaramiento SALT es opcional y puede ser omitida del procedimiento de autentificación. En tal caso, no se introduce ninguna instancia aleatoria SALT en la función de enmascaramiento *f* para calcular la respuesta esperada enmascarada XRES' y la respuesta de usuario enmascarada RES', respectivamente. Sin embargo, con el fin de aumentar la seguridad y, en particular, para detener ataques previos a la computación, la instancia aleatoria de enmascaramiento SALT está incluida, preferiblemente, como entrada de la función de enmascaramiento. De esta forma, la instancia aleatoria de enmascaramiento SALT puede ser generada como un valor completamente aleatorio en el centro de autentificación y subsiguientemente transmitida a la parte intermediaria conjuntamente con la respuesta esperada enmascarada XRES' y la instancia aleatoria RAND. Sin embargo, con el fin de evitar un intercambio adicional de señales entre el centro de autentificación y la parte intermediaria, la instancia aleatoria de enmascaramiento SALT puede, alternativamente, ser deducida de la instancia aleatoria RAND. En este caso, el centro de autentificación genera, preferiblemente, la instancia aleatoria de enmascaramiento SALT por medio de alguna función *h* de la instancia aleatoria RAND. En consecuencia, no es necesario transmitir ninguna instancia aleatoria de enmascaramiento SALT a la parte intermediaria, la cual, en lugar de ello, puede utilizar la misma función *h* para generar la instancia aleatoria de enmascaramiento SALT a partir de la instancia aleatoria RAND. Un ejemplo de instancia aleatoria enmascarada SALT que se puede utilizar consiste simplemente en reutilizar la instancia aleatoria RAND como instancia aleatoria enmascarada SALT, de tal manera que *h* se representa como una función unidad.

La función *h* puede ser una función pública o una función asociada y distribuida con el acuerdo comercial entre la parte intermediaria y la parte legal (tal como un operador doméstico) del centro de autentificación, del cual se discutirán en detalle diversos aspectos más adelante.

La función de enmascaramiento *f* utilizada, por un lado, por el centro de autentificación para generar la respuesta esperada enmascarada y, por otro lado, por la parte intermediaria para calcular la respuesta de usuario enmascarada, puede ser una función en un solo sentido o no invertible, y/o distributiva. De preferencia, la función de enmascaramiento es una función distributiva criptográfica que tiene una aplicación funcional en un solo sentido o no invertible y propiedades que hacen que no sea posible encontrar dos entradas diferentes que se fragmenten en un valor común.

Para información adicional sobre funciones no invertibles y funciones distributivas, se hace referencia a la divulgación de A. J. Menezes, P. C. van Oorschot y S. C. Vanstone: "*Handbook of Applied Cryptography*" ("Manual de criptografía aplicada"), CRC Press, capítulo 1, págs. 1-48.

La función de enmascaramiento *f* puede ser una función pública o una función privada conocida por el centro de autentificación y por la parte intermediaria. En este último caso, la función de enmascaramiento privada puede estar asociada con un acuerdo comercial entre la parte legal, tal como un operador doméstico dado, del centro de autentificación y la parte intermediaria, tal como un proveedor de servicios. Si la parte legal del centro de autentificación, por ejemplo, un operador doméstico, tiene semejante acuerdo comercial con diversos proveedores de servicios diferentes, puede utilizarse una función privada correspondiente por parte del operador doméstico para cada proveedor de servicios, es decir, cada acuerdo de operador-proveedor se plasma en una función de enmascaramiento privada. Sin embargo, de forma alternativa, es posible utilizar una misma función de enmascaramiento pública para todos los proveedores de servicios.

Si se conoce la función de enmascaramiento, es posible, al menos en teoría, buscar una respuesta de usuario que haga que la función de enmascaramiento realice una evaluación en la respuesta esperada enmascarada recibida desde el centro de autentificación. Una parte intermediaria malintencionada, tal como un proveedor de servicios, puede entonces desplegar dicho ataque para "demostrar" que un usuario ha sido autentificado incluso si no se ha llevado a cabo ninguna autentificación del usuario. Esto se resuelve simplemente por una elección cuidadosa de las propiedades de los parámetros de autentificación. Por ejemplo, si se escoge la respuesta del usuario de manera que sea de *n* bits y la respuesta esperada enmascarada de forma que sea de *m* bits, con $n > m$, el número promedio de respuestas de usuario que se han de comprobar antes de encontrar la que está asociada con una respuesta esperada enmascarada presente, es aproximadamente 2^{m-1}. Además, la probabilidad de que esta sea la respuesta de usuario correcta es solo de $2^{-(n-m)}$. Para un sistema de comunicaciones móviles UMTS, los tamaños de parámetros normalizados permiten que *n* sea 96 y *m* sea 80, lo que da lugar a la tarea imposible de comprobar 2^{79} respuestas de usuario diferentes y a una probabilidad de respuesta de usuario correcta de solo 2^{-16}.

Es también posible enmascarar la respuesta de usuario / respuesta esperada de manera diferente dependiendo, por ejemplo, del servicio real que se obtiene de la parte intermediaria. Esto significa que para algunos se utiliza un cierto tipo de enmascaramiento, por ejemplo, una primera función de enmascaramiento, mientras que para otros servicios se emplea una segunda función de enmascaramiento diferente. En tal caso, se incluye preferiblemente alguna forma de información en la transmisión entre el centro de autentificación la parte intermedia con el fin de notificar la función de enmascaramiento que se ha de utilizar en la autentificación de usuario particular.

Con el fin de permitir una suave migración en relación con la infraestructura existente, se informa, preferiblemente, a la parte intermediaria sobre si se ha empleado o no la función de enmascaramiento a la hora de calcular la respuesta esperada distribuida. De esta forma, el protocolo para la distribución de parámetros de autentificación es, preferiblemente, extendido o ampliado con tal indicación. Similarmente, puede incluirse en el protocolo una indicación acerca de qué función de enmascaramiento utilizar, si está presente una elección entre diferentes funciones de enmascaramiento, tal y como se ha explicado anteriormente.

La parte intermediaria puede utilizar la respuesta recibida del usuario y alguna otra información de identificación de usuario, tal como una ID de usuario, preferiblemente junto con la instancia aleatoria utilizada para generar la respuesta, como información de prueba para demostrar que este usuario concreto ha sido realmente autentificado. De esta forma, la parte intermediaria almacena convenientemente la respuesta de usuario recibida, la ID de usuario y la instancia aleatoria en una posición adecuada para su recuperación ulterior, en caso necesario, como evidencia de la autentificación del usuario. En este procedimiento sin conexión o fuera de línea para la demostración de la autentificación del usuario, la respuesta del usuario y la ID del usuario, preferiblemente junto con la instancia aleatoria correspondiente, pueden ser almacenadas en la parte intermediaria, en alguna otra posición accesible.

Cuando es instada por el centro de autentificación o por alguna otra parte relacionada, para que proporcione pruebas de la autentificación de un usuario dado, la parte intermediaria puede transmitir la información de prueba, tal como la respuesta RES de usuario, la instancia aleatoria RAND correspondiente y la ID de usuario al centro de autentificación. Preferiblemente, el centro de autentificación recupera entonces la clave secreta K_i asociada con el usuario dado y calcula el valor de respuesta esperado XRES basándose en la RAND recibida y en la clave secreta K_i, y, finalmente, compara el valor RES recibido con el valor XRES calculado a fin de verificar si el usuario ha sido realmente autentificado en la parte intermediaria. Si el valor RES coincide con el valor XRES, la información de prueba se considera válida.

Parte intermediaria: RAND, RES, ID de usuario

Centro de autentificación: ID de usuario $\Rightarrow$ XRES

$$g(K_i, \text{RAND}) \Rightarrow \text{XRES}$$

$$\text{comprobación: XRES} \stackrel{?}{=} \text{RES}$$

Alternativamente, la parte intermediaria transmite simplemente el valor RES y la ID de usuario de un usuario dado a la parte intermediaria. En este caso, el centro de autentificación necesita, típicamente, almacenar valores XRES, o valores RAND, de tal manera que los valores XRES correspondientes puedan ser calculados para los usuarios de modo que pueda realizar una comparación entre RES y XRES.

Si se desea un procedimiento bajo conexión o en línea, la respuesta de usuario y la ID de usuario, preferiblemente junto con la instancia aleatoria correspondiente, son remitidas más o menos directamente desde la parte intermediaria al centro de autentificación, con lo que se hace posible la demostración de la autentificación.

Asociación de Información de prueba de autentificación a una parte intermediaria específica

Una amenaza adicional es que una parte intermediaria malintencionada envíe pueda enviar la información de prueba a otra parte que, a su vez, presente la información de prueba al centro de autentificación en una petición de pago (suponiendo, por ejemplo, que los servicios de la otra parte son más caros que los de la parte intermediaria). Además, puede ser también posible que un atacante lea la información de prueba, incluyendo, por ejemplo, la ID de usuario, la respuesta RES de usuario y la instancia aleatoria correspondiente RAND, desde un nodo ilegítimamente intervenido de la parte intermediaria. Este atacante podría entonces presentar la información de prueba recibida al centro de autentificación, afirmando falsamente que el usuario ha accedido a algún servicio y solicitando un pago. Si se considera necesario o de otra forma importante, este problema concreto puede resolverse asociando datos de autentificación, generados en el centro de autentificación para un usuario dado, con la parte intermediaria que participa en la autentificación de usuario con el fin de vincular la información de prueba correspondiente con la parte intermediaria.

En las etapas iniciales del procedimiento de autentificación global de la invención, la parte intermediaria remite una ID de usuario, conjuntamente con una petición de datos de autentificación, al centro de autentificación. En general, la ID de usuario está acompañada por información que identifica la parte intermediaria que solicita datos de autentificación. A fin de permitir una vinculación ulterior de información de prueba de autentificación a una parte intermediaria específica, el centro de autentificación puede almacenar la ID de usuario y los datos de autentificación generados, tales como la RAND, la SALT y/o la XRES, con una referencia sobre a qué parte intermedia han sido enviados los datos de autentificación. Si se interrelacionan, en el centro de autentificación, al menos parte de los datos de autentificación generados para un usuario dado con una identificación de la parte intermediaria que solicitó los datos de autentificación, la información de prueba correspondiente no puede ser utilizada por ninguna otra parte.

Cuando la parte intermediaria es instada a proporcionar información de prueba ante el centro de

autentificación, este también transmite su propia identidad, a la que se hace referencia también como identidad de proveedor de servicios, denotada como ID_{SP}, al centro de autentificación. Al recibir información de prueba, el centro de autentificación compara la respuesta RES de usuario obtenida de la parte intermediaria con una respuesta esperada XRES almacenada o regenerada, a fin de verificar que un usuario ha sido autentificado. Sin embargo, el centro de autentificación puede ahora comparar también información de prueba recibida con datos de autentificación almacenados, teniendo una referencia con respecto a la parte intermediaria a la que fueron transmitidos los datos de autentificación, al objeto de verificar si la información de prueba está realmente asociada con la parte intermedia que *presenta* la información de prueba.

Otra posible solución para vincular información de prueba a una parte intermediaria consiste en asociar la *generación* de la instancia aleatoria de enmascaramiento SALT ubicada en el centro de autentificación con la parte intermediaria ID_{SP}. El centro de autentificación puede tener un conjunto de funciones *h* diferentes que se utilizan para generar SALT a partir de RAND, y, preferiblemente, asigna a cada parte intermediaria una función única o exclusiva h_{SP}. Esta función h_{SP} es utilizada por el centro de autentificación para generar la instancia aleatoria de enmascaramiento SALT a partir de la RAND, y la SALT generada es transmitida a la parte intermediaria. A medios que se almacenen los valores de SALT con una referencia a la ID_{SP} correspondiente en el centro de autentificación, las funciones h_{SP} se mantienen, preferiblemente, en secreto por parte del centro de autentificación. Cuando se presenta información de prueba, incluyendo RES, RAND e ID de usuario, al centro de autentificación, la parte intermediaria es también requerida para que transmita su ID_{SP} asociada y la instancia aleatoria de enmascaramiento SALT previamente recibida. Basándose en la ID_{SP} recibida, el centro de autentificación identifica una función h_{SP} relevante y calcula una instancia aleatoria de enmascaramiento esperada XSALT basándose en la instancia aleatoria RAND recibida. A fin de verificar que la información de prueba se origina en la parte intermediaria correcta, XSALT se compara con la SALT recibida desde la parte intermediaria. Una coincidencia entre ellas es una verificación o corroboración del origen correcto de la información de prueba. El hecho de mantener la función única específica de parte intermedia en secreto hace imposible que otra parte pueda utilizar la información de prueba.

Parte intermediaria: RAND, SALT, RES, ID de usuario, ID_{SP}

Centro de autentificación: ID de usuario $\Rightarrow K_i$

$$g(K_i, RAND) \Rightarrow XRES$$

$$ID_{SP} \Rightarrow h_{SP}$$

$$h_{SP}(RAND) \Rightarrow XSALT$$

comprobaciones:

$$XRES \stackrel{?}{=} RES$$

$$XSALT \stackrel{?}{=} SALT$$

En lugar de utilizar una función h_{SP} única para parte intermediaria en la generación de la instancia aleatoria de enmascaramiento SALT, es posible utilizar una función común *h* por parte del centro de autentificación para diversas partes intermedias o todas ellas. Sin embargo, la función *h* tiene como entradas tanto la instancia aleatoria RAND como la ID_{SP} de parte intermedia. De esta forma, el centro de autentificación calcula la SALT basándose en la ID_{SP} recibida, junto con la ID de usuario, en las etapas iniciales del procedimiento de autentificación. De la misma manera que se ha descrito anteriormente, se solicita a la parte intermedia que incluya la ID_{SP} y una copia de la SALT recibida en la información de prueba. Una vez recibida, el centro de autentificación calcula una instancia aleatoria de enmascaramiento esperada XSALT basándose en la ID_{SP} y en la RAND recibidas, y en la función *h*. XSALT se compara entonces con la SALT transmitida desde la parte intermediaria, y una coincidencia entre ellas verifica el correcto origen de la información de prueba. El hecho de mantener la función común *h* en secreto hace imposible que otra parte pueda presentar información de prueba válida basándose solo en la RES y la RAND.

Parte intermediaria: RAND, SALT, RES, ID de usuario, ID_{SP}

Centro de autentificación: ID de usuario $\Rightarrow K_i$

$$g(K_i, RAND) \Rightarrow XRES$$

$$h(RAND, ID_{SP}) \Rightarrow XSALT$$

comprobaciones:

$$XRES \stackrel{?}{=} RES$$

$$XSALT \stackrel{?}{=} SALT$$

En aún otra realización alternativa, la generación de la instancia aleatoria RAND puede estar basada en la ID_{SP} de la parte intermedia. Al solicitarse una autentificación de usuario, el centro de autentificación genera una preinstancia aleatoria RAND' y calcula la instancia RAND por medio de la RAND' y de la ID_{SP} de la parte intermedia, como entradas para una función *r*.

$$RAND = r(ID_{SP}, RAND')$$

Esta instancia aleatoria RAND es subsiguientemente utilizada para generar la respuesta esperada RES y es enviada a la parte intermedia junto con la respuesta esperada enmascarada XRES'. El centro de autentificación almacena RAND' con una referencia a la ID de usuario asociada y a la ID_{SP} de la parte intermediaria. A la hora de verificar que un usuario ha sido ciertamente autentificado por la parte intermediaria, el centro de autentificación calcula una instancia aleatoria esperada XRAND con la ID_{SP} y la RAND' almacenada, como entradas para la función *r*. XRAND es entonces comparada con la RAND recibida desde la parte intermedia, y si coinciden, el centro de autentificación puede verificar que la información de prueba es transmitida desde la parte intermediaria correcta. También se lleva a cabo la verificación de la autentificación del usuario por medio de la RES y la XRES, como sigue. Esta solución es especialmente aplicable cuando no se emplea ninguna instancia aleatoria de enmascaramiento SALT en el procedimiento de autentificación del usuario.

Parte intermediaria: RAND, RES, ID de usuario, ID_{SP}

Centro de autentificación: ID de usuario $\Rightarrow K_i$

$$g(K_i, RAND) \Rightarrow XRES$$

$$ID_{SP} \Rightarrow RAND'$$

$$r(RAND', ID_{SP}) \Rightarrow XRAND$$

comprobaciones:

$$XRES \stackrel{?}{=} RES$$

$$XRAND \stackrel{?}{=} RAND$$

Las funciones anteriormente expuestas *h*, h_{SP} y *r* tienen, preferiblemente, una aplicación funcional en un solo sentido o no invertible, con propiedades que hacen imposible encontrar dos entradas diferentes que se fragmenten en un valor común.

En general, la comparación de XRES-RES verifica si un usuario dado, con una ID de usuario, ha sido autentificado, y la comparación de XSALT-SALT / XRAND-RAND verifica si el usuario ha sido autentificado por la parte intermediaria que tiene la identidad ID_{SP}.

Aspectos criptográficos opcionales

Si bien no se ha ilustrado en la Figura 4, puede generarse información adicional, tal como una clave de confidencialidad, una clave de integridad y una ficha de autentificación, en el centro de autentificación, y transmitirse a la parte intermediaria. En tal caso, esta información adicional, por ejemplo, la clave de confidencialidad y la clave de integridad, pueden ser modificadas por la respuesta antes de su uso. Por ejemplo, el centro de autentificación puede proteger criptográficamente la clave de confidencialidad y la clave de integridad basándose en la respuesta esperada calculada. Las claves se transmiten entonces encriptadas o cifradas a la parte intermediaria, la cual lleva a cabo cualquier intercepción de las claves distribuidas que no son de utilidad para la conexión secreta o pinchado de cable y el desciframiento. La parte intermediaria extrae entonces la clave de confidencialidad y la clave de integridad de la información cifrada utilizando la respuesta recibida del usuario.

Además, puede protegerse criptográficamente otra información distinta de las claves obtenidas del AKA, por medio de la respuesta esperada, antes de ser transmitidas entre el centro de autentificación y la parte intermediaria.

En general, la transmisión de parámetros de autentificación, incluyendo la respuesta esperada enmascarada, la instancia aleatoria y la instancia aleatoria enmascarada, entre el centro de autentificación y la parte intermediaria, puede ser protegida criptográficamente. En aplicaciones de UMTS, por ejemplo, puede utilizarse el protocolo MAPSec para la protección de los parámetros.

Aspectos de aplicación práctica

Las etapas, acciones y algoritmos anteriormente descritos pueden ser implementados en software / hardware o en cualquier combinación de estos. Para implementaciones en dispositivos físicos o hardware, puede utilizarse tecnología de ASIC (Circuito Integrado Específico de la Aplicación –"Application Specific Integrated Circuit") o cualquier otra tecnología de circuitos convencional. Aunque puede preferirse un hardware especial, resistente a la manipulación indebida, por razones de seguridad, son a menudo más convenientes las implementaciones de software adecuadamente protegido.

La Figura 6 ilustra esquemáticamente un ejemplo de un centro de autentificación de acuerdo con una realización preferida de la invención. El centro de autentificación 50 incluye, generalmente, una unidad 10 de algoritmo de autentificación, destinada a generar datos de autentificación que se emplean para autentificar a un usuario, una unidad 20 de verificación de prueba y una base de datos 30. La unidad 10 de algoritmo de autentificación comprende un generador 12 de datos de instancia, un generador 14 de XRES y una unidad 16 de función de enmascaramiento. Como su propio nombre indica, el generador 12 de datos de instancia genera datos de instancia, incluyendo la instancia aleatoria y, opcionalmente, también la instancia aleatoria de enmascaramiento. El generador 14 de XRES genera la respuesta esperada XRES basándose en los datos de instancia y en una clave secreta asociada al usuario, procedente de la base de datos 30. La unidad 16 de función de enmascaramiento genera la respuesta esperada enmascarada basándose en la instancia aleatoria de enmascaramiento opcional y en la respuesta esperada, procedentes, respectivamente, del generador 12 de datos de instancia y el generador 14 de XRES. La unidad 20 de verificación de prueba se implementa también, preferiblemente, en el centro de autentificación 50 para verificar la información de prueba recibida de la parte intermediaria.

Esta unidad 20 de verificación de prueba utiliza, preferiblemente, datos almacenados en la base de datos 30 para la verificación de prueba. La base de datos 30 puede incluir, opcionalmente, además de información sobre la ID de usuario y la clave secreta K_i asociada, datos de autentificación y/o datos semejantes almacenados con referencia a información ID_{SP} de identificación de parte intermediaria. El centro de autentificación 50 también comprende un transmisor / receptor 40, con sus circuitos asociados, para la comunicación con la parte intermediaria y con el usuario.

La Figura 7 ilustra esquemáticamente un ejemplo de una parte intermediaria de acuerdo con una realización preferida de la invención. La parte intermediaria 200 incluye una unidad 210 de algoritmo de autentificación para la autentificación del usuario. La unidad 210 de algoritmo de autentificación comprende un generador 212 de respuesta enmascarada y una unidad de comparación 214. El generador 212 de respuesta enmascarada genera una respuesta de usuario enmascarada basándose en una función de enmascaramiento y en la respuesta de usuario recibida del usuario. La unidad de comparación 214 se emplea para comparar la respuesta de usuario enmascarada procedente del generador 212 con la respuesta esperada enmascarada que se transmite desde el centro de autentificación. También se ha dispuesto, preferiblemente, una unidad de almacenamiento / remisión 270 en la parte intermediaria 200, a fin de almacenar y/o remitir información de prueba que incluye la respuesta del usuario y la ID de usuario, así como también, preferiblemente, datos de instancia recibidos desde el centro de autentificación o generados por la unidad 210 de algoritmo de autentificación. Esta información de prueba procedente de la unidad de almacenamiento y/o remisión 270 es transmitida al centro de autentificación, por ejemplo, bajo petición o tan pronto como se obtenga la información de prueba por la parte intermediaria 200. La parte intermediaria 200 también comprende un transmisor / receptor 240 con sus circuitos asociados, para la comunicación con el centro de autentificación y con el usuario.

Ejemplo de aplicación – sistema de comunicación móvil

Si bien la invención es aplicable, generalmente, a cualquier sistema de respuesta ante instancia de clave secreta, la invención ha resultado ser particularmente útil en sistemas de comunicación móvil. La invención se describirá a continuación con referencia a una aplicación y una particulares proporcionadas a modo de ejemplo, a saber, un sistema de comunicación móvil en el cual la parte intermediaria es un nodo de red que gestiona una red móvil / celular dentro de la cual se está desplazando de forma itinerante una unidad móvil (usuario). En este ejemplo particular, el centro de autentificación es un centro de autentificación (AuC –"authentication center") de operador doméstico. La unidad móvil está asociada, por ejemplo, a través de una suscripción o una cuenta de prepago, con un operador doméstico que gestiona un sistema de red doméstico. Esta relación de usuario-operador se plasma, típicamente, en una tarjeta de SIM de las que se utilizan en las unidades móviles de GSM, o en una tarjeta de SIM de UMTS (USIM –"UMTS SIM") de las que se utilizan en las unidades móviles de UMTS. Debe comprenderse, sin embargo, que en una aplicación de comunicaciones móviles más general, la parte intermediaria puede ser cualquier tipo de proveedor de servicios, incluyendo un nodo de red visitada, el propio nodo de MSC / VLR del operador doméstico, un proveedor de servicios de web, un proveedor de contenidos de medios de soporte de información, así como un corredor de pagos.

La Figura 8 es un diagrama de bloques esquemático de una realización proporcionada a modo de ejemplo de un sistema de autentificación, que se ilustra como un sistema de red doméstica con una unidad móvil asociada que se está desplazando de forma itinerante dentro de un sistema de red visitado. El sistema doméstico 100 comprende, generalmente, uno o más nodos 160 de red, de los cuales se ha ilustrado uno. Por ejemplo, el nodo 160 de red puede consistir en un MSC (Centro de Conmutación Móvil –"Mobile Switching Center") o en una estación de base

(BS –“base station”). En el ejemplo de la Figura 8, el nodo 160 de red comprende un HLR (Registro de Posiciones Domésticas) 130. Este HLR 130 incluye información, por ejemplo, ID de usuario y clave de suscripción secreta K_i correspondiente, de los usuarios asociados al sistema doméstico 100. El HLR 130 puede incluir, opcionalmente, datos de autentificación y/o datos semejantes almacenados con referencia a la identificación de parte intermediaria. Además, el nodo 160 de red comprende también un centro de autentificación (AuC) 150 que gestiona y participa en la autentificación de los usuarios. El AuC 150 comprende una unidad 10 de algoritmo de autentificación que implementa un algoritmo de autentificación, así como una unidad 20 de verificación de prueba, destinada a la verificación de información de prueba procedente del sistema visitado 200. Cuando se ejecuta, el algoritmo de autentificación genera los datos de autentificación relevantes de la invención. El nodo 160 de red doméstica está equipado, adicionalmente, con un transmisor / receptor 140, con sus circuitos asociados, para transmitir la instancia aleatoria generada, la respuesta esperada enmascarada y, posiblemente, la instancia aleatoria enmascarada, a un nodo 260 de red de un sistema visitado o recorrido de forma itinerante 200.

El sistema visitado 200 comprende, de la misma manera, uno o más nodos 260 de red, de los cuales se ha ilustrado uno en la Figura 8. El nodo 260 de red del sistema visitado 200 comprende, preferiblemente, un VLR (Registro de Posiciones Visitadas) 230 y un algoritmo de autentificación 210. Por otra parte, se ha dispuesto un transmisor / receptor 240 para recibir los parámetros de autentificación desde el sistema doméstico 100 y remitir la instancia aleatoria recibida a la unidad móvil en desplazamiento itinerante 400, así para transmitir información de prueba al centro de autentificación 150 del sistema doméstico.

El nodo 260 de red visitada comprende también, preferiblemente, una unidad de almacenamiento y/o remisión 270 destinada a almacenar la respuesta de usuario recibida desde la unidad móvil 400 y, posiblemente, la instancia aleatoria procedente del sistema doméstico 100. Sin embargo, el almacenamiento de la respuesta de usuario puede, como alternativa o de forma complementaria, proporcionarse en otra ubicación a la que puede accederse por parte del operador del sistema visitado 200 para una ulterior recuperación de la información en un procedimiento de prueba de autentificación de usuario. Los datos almacenados en esta unidad 260 son transmitidos al centro de autentificación al ser solicitados por este.

En el ejemplo particular de la Figura 8, el usuario es una unidad móvil itinerante 400 que está siendo autentificada por un nodo 260 de red del sistema de red 200 que es recorrido de forma itinerante o visitado. Tal y como se ha mencionado anteriormente, la unidad móvil 400 comprende, preferiblemente, un SIM (USIM) 480 equipado con la clave secreta K_i 415 y una unidad 410 de algoritmo de autentificación. Este algoritmo de autentificación implementado en la unidad 410 puede ser, por ejemplo, el algoritmo A3 del protocolo de AKA en GSM y en UMTS. Cuando se ejecuta, el algoritmo de autentificación calcula una respuesta de usuario basándose, preferiblemente, en la instancia aleatoria remitida desde el sistema visitado 200 y en la clave secreta K_i del SIM 480. La unidad móvil 400 envía entonces la respuesta del usuario al nodo 260 de red del sistema visitado, donde se lleva a cabo la autentificación final.

La Figura 9 ilustra otra realización proporcionada a modo de ejemplo de un sistema de red doméstico 300 que incluye un AuC 150 de acuerdo con la invención. En esta realización, el sistema doméstico 300 se ha ilustrado con dos nodos 360, 356 de red, cada uno de los cuales está equipado con un transmisor / receptor 340, 345 respectivo. Un primer nodo 360 comprende el HLR 130, en tanto que el AuC 150, con la unidad 10 de algoritmo de autentificación y los medios 20 de verificación de prueba, está dispuesto en un segundo nodo 365. El primer nodo 360 puede ser un MSC, de manera que el segundo nodo 365 se materializa como una BS. Alternativamente, tanto el primer nodo 360 como el segundo nodo 365 pueden ser MSC o BS, o bien el primer nodo 360 puede ser una BS y el segundo nodo 365 un MSC.

La Figura 10 es un diagrama de bloques esquemático de aún otra realización proporcionada a modo de ejemplo de un sistema de red doméstico de acuerdo con la invención, de tal manera que el algoritmo de autentificación doméstico está distribuido entre diversos nodos de red. En la Figura 10 se han ilustrado explícitamente dos nodos 560, 565 de red. En esta realización, el AuC 550 está distribuido entre los dos nodos 560, 565. Esto significa que la parte 510 del algoritmo de autentificación global se ha implementado en el primer nodo 560, en tanto que la parte restante 515 del algoritmo de autentificación se ha implementado en un segundo nodo 565, o en diversos otros nodos. La unidad 20 de verificación de prueba del AuC 550 se ha implementado, preferiblemente, en el nodo 560 de red que está alojando el HLR 130, por lo que tiene acceso a los datos almacenados en el HLR 130.

El sistema visitado puede, de la misma manera, tener el VLR y el algoritmo de autentificación repartidos en diferentes nodos de red, y/o tener el algoritmo de autentificación distribuido entre diferentes nodos.

Para información detallada adicional sobre procedimientos de autentificación generales en sistemas de comunicación móvil, se hace referencia a la divulgación de J. Arkko y H. Haverinen: “*EAP AKA Authentication*” (“Autentificación de AKA de EAP”), Internet Draft of the Internet Engineering Task Force [Borrador en Internet del Grupo de Trabajo de Ingeniería de Internet], y al Borrador de Internet previamente mencionado: “*EAP SIM Authentication*” (“Autentificación de SIM de EAP”), por H. Haverinen.

Ejemplo – Un corredor actuando como centro de autentificación

Como se ha indicado anteriormente, el centro de autentificación no es, necesariamente, el centro de

autentificación de un operador doméstico particular, sino que puede ser un corredor 750 que actúa como un centro de autentificación general, o centro de identidad, para un cierto número de operadores de red diferentes, tal y como se ha ilustrado esquemáticamente en la Figura 11. En este caso, al corredor 750 del centro de autentificación, o centro de identidad, se le confían, generalmente, la información de identificación de usuario y la información de clave secreta 730, 735 procedentes de los distintos operadores de red, haciendo de este modo posible que el corredor 750 ayude a la autentificación de usuarios en diversas partes intermedias 200-1 a 200-N.

Generalmente, cuando un/a usuario/a 400 desea autentificarse a sí mismo/a ante una parte intermediaria 200 dada, el usuario envía su ID de usuario y, si se le requiere, alguna información que representa la identidad ID_{OP} del operador doméstico, a la parte intermediaria. La parte intermediaria remite entonces la ID de usuario y la ID_{OP}, junto con información que identifica la ID_{SP} de la parte intermediaria, al corredor 750 del centro de autentificación, en una petición de datos de autentificación. El corredor 750 del centro de autentificación identifica, basándose en la ID_{OP} y la ID de usuario recibidas, la clave secreta K_i asociada con el usuario 400 y, a continuación, genera los datos de autentificación (enmascarados) de acuerdo con el algoritmo de autentificación de la invención. El resto del procedimiento de autentificación (y verificación de prueba) corresponde esencialmente a la anterior descripción de la invención.

En un escenario o contexto típico, el usuario 400 necesita, en primer lugar, autentificarse ante su propio operador, y envía, por tanto, su ID de usuario al nodo de MSC / VLR (que actúa aquí como parte intermediaria) del operador doméstico, el cual remite la ID de usuario y su propia ID al corredor 750 del centro de autentificación, en una petición de datos de autentificación. El corredor 750 del centro de autentificación genera los datos de autentificación requeridos para la autentificación. Una vez que el usuario ha sido finalmente autentificado, el MSC / VLR puede almacenar la información de prueba correspondiente para su ulterior recuperación, en caso necesario, como evidencia de la autentificación del usuario. Si el usuario desea, subsiguientemente, acceder, por ejemplo, a algún servicio de web ofrecido por un proveedor de servicios de web, se le solicita al usuario que transmita su ID de usuario e información representativa de la identidad ID_{OP} del operador domestico al proveedor de servicios de web. Si el proveedor de servicios de web es independiente (otra parte intermediaria) del operador doméstico, puede, no obstante, tener una cierta relación con el operador doméstico y preguntar al operador doméstico acerca de información sobre si el usuario ha sido autentificado. Alternativamente, el proveedor de servicios de web transmite la ID_{OP} y la ID de usuario al corredor 750 en su propia petición de datos de autentificación, y almacena más tarde su propia información de prueba. De forma correspondiente, puede llevarse a cabo un procedimiento similar para un proveedor de contenidos, un nodo de red visitada o cualquier otra parte intermediaria.

Puede emplearse también un corredor que actúe como un centro de autentificación general para deducir claves para la encriptación o cifrado de extremo a extremo entre un usuario y una parte intermediaria. En tal caso, estas claves deducidas pueden mantenerse en secreto desde el operador de red. El usuario puede entonces obtener la clave de cifrado de extremo a extremo, por ejemplo, en una suscripción a los servicios ofrecidos por la parte intermediaria o con el pago de servicios utilizados.

Las realizaciones anteriormente descritas se han proporcionado meramente a modo de ejemplos, y ha de comprenderse que la presente invención no está limitada por ellas. Las reivindicaciones que se acompañan definen el ámbito de la invención.

REIVINDICACIONES

1. Un método basado en instancia-respuesta para la autentificación de un usuario en un sistema de comunicaciones, el cual tiene al menos el usuario asociado con un centro de autentificación, **caracterizado por** las etapas de:

- generar (S12), en el centro de autentificación (50, 150, 550), una respuesta esperada por medio de una función de respuesta (14), a partir de una clave secreta, compartida con el usuario, y una instancia aleatoria (S11);

- generar (S14), en dicho centro de autentificación, una respuesta esperada enmascarada por medio de una función de enmascaramiento (16), en respuesta a dicha respuesta esperada;

- transmitir (S21) dicha respuesta esperada enmascarada y dicha instancia aleatoria a una parte intermedia o intermediaria (200);

- de manera que la parte intermediaria transmite (S31) dicha instancia aleatoria al usuario (400);

- generar (S32), en dicho usuario, una respuesta por parte de dicha función de respuesta en respuesta a dicha clave secreta y a dicha instancia aleatoria;

- transmitir (S33) dicha respuesta de usuario a dicha parte intermediaria; generar (S42), en dicha parte intermediaria, una respuesta de usuario enmascarada por medio de la misma función de enmascaramiento que la de dicho centro de autentificación, en respuesta a dicha respuesta de usuario;

- de tal modo que dicha parte intermedia autentifica al usuario en respuesta a un resultado positivo de la verificación de que dicha respuesta de usuario enmascarada corresponde a dicha respuesta esperada enmascarada (S51, D52).

2. El método de acuerdo con la reivindicación 1, **caracterizado por** la etapa adicional de que dicha parte intermediaria (200) gestiona la información de prueba de autentificación, incluyendo al menos dicha respuesta de usuario recibida desde dicho usuario (400) e información de identificación de usuario correspondiente, a fin de permitir que dicha parte intermediaria demuestre que dicho usuario ha sido identificado.

3. El método de acuerdo con la reivindicación 2, **caracterizado por que** dicha información de prueba de autentificación incluye, adicionalmente, dicha instancia aleatoria.

4. El método de acuerdo con la reivindicación 1, **caracterizado por que** dichas etapas de generar una respuesta esperada enmascarada y generar una respuesta de usuario enmascarada se llevan a cabo también en respuesta a una instancia aleatoria de enmascaramiento común para una seguridad incrementada.

5. El método de acuerdo con la reivindicación 4, **caracterizado por que** dicha instancia aleatoria de enmascaramiento se deduce dicha instancia aleatoria recibida.

6. El método de acuerdo con la reivindicación 2, **caracterizado por** las etapas adicionales de:

- transmitir, por dicha parte intermediaria (200), información de prueba de autentificación a dicho centro de autentificación (50, 150, 550); y

- verificar, por parte de dicho centro de autentificación, si dicho usuario ha sido autentificado en dicha parte intermediaria basándose en dicha información de prueba recibida.

7. El método de acuerdo con la reivindicación 6, **caracterizado por que** dicha etapa de verificación comprende la etapa de comparar la respuesta de usuario de dicha información de prueba recibida con una respuesta esperada correspondiente proporcionada por dicho centro de autentificación.

8. El método de acuerdo con la reivindicación 7, **caracterizado por que** dicha información de prueba de autentificación incluye, adicionalmente, dicha instancia aleatoria, y dicho método comprende, adicionalmente, las etapas de recuperar, en dicho centro de autentificación, dicha clave secreta basándose en dicha identificación de usuario, y volver a computar dicha respuesta esperada a partir de dicha clave secreta recibida y dicha instancia aleatoria.

9. El método de acuerdo con la reivindicación 2, **caracterizado por** la etapa adicional de asociar a dicha parte intermediaria datos de identificación generados para un usuario dado, por parte de dicho centro de autentificación, a fin de vincular a dicha parte intermediaria información de prueba correspondiente.

10. El método de acuerdo con la reivindicación 9, **caracterizado por que** dichos datos de autentificación están interrelacionados, en dicho centro de autentificación, con información de identificación que identifica dicha parte intermediaria, y dichos datos de autentificación son subsiguientemente comparados, en dicho centro de autentificación, con una representación de información de prueba recibida, con el fin de verificar que dicha información de prueba está asociada con dicha parte intermediaria.

11. El método de acuerdo con la reivindicación 10, **caracterizado por que** dichos datos de autentificación incluyen al menos una de dicha instancia aleatoria, dicha respuesta esperada y una instancia aleatoria de enmascaramiento utilizada para generar dicha respuesta esperada enmascarada y dicha respuesta de usuario enmascarada.

12. El método de acuerdo con la reivindicación 10, **caracterizado por que** dichos datos de autentificación incluyen datos de instancia aleatoria, y la generación de dichos datos de instancia está interrelacionada con dicha parte intermediaria.

13. El método de acuerdo con la reivindicación 12, **caracterizado por que** dichos datos de instancia son generados por una función que es única o exclusiva para dicha parte intermediaria.

14. El método de acuerdo con la reivindicación 12, **caracterizado por que** dichos datos de instancia se generan basándose en información de identificación que identifica dicha parte intermediaria.

15. El método de acuerdo con la reivindicación 1, **caracterizado por** las etapas adicionales de:

- encriptar o cifrar datos transmitidos desde dicho centro de autentificación a dicha parte intermediaria por medio de dicha respuesta esperada; y

- desencriptar o descifrar dichos datos cifrados en dicha parte intermediaria por medio de dicha respuesta de usuario recibida.

16. El método de acuerdo con la reivindicación 1, **caracterizado por que** dicho centro de autentificación y dicha parte intermediaria están situados en nodos (260, 160) de red de un sistema de comunicaciones móviles.

17. El método de acuerdo con la reivindicación 1, **caracterizado por que** dicho centro de autentificación es un corredor (750) que actúa como un centro de autentificación general, o centro de identidad.

18. Un sistema de autentificación de usuario basado en respuesta ante instancia, para un sistema de comunicaciones, que tiene al menos un usuario (400) asociado con un centro de autentificación (50, 150, 550), **caracterizado por**:

- medios (14) para generar, en el centro de autentificación, una respuesta esperada por medio de una función de respuesta a partir de una clave secreta, compartida con el usuario, y una instancia aleatoria;

- medios (16) para generar, en dicho centro de autentificación, una respuesta esperada enmascarada por medio de una función de enmascaramiento, en respuesta a dicha respuesta esperada;

- medios (40), situados en dicho centro de autentificación, para transmitir dicha respuesta esperada enmascarada y dicha instancia aleatoria a una parte intermediaria;

- medios (240), situados en la parte intermediaria, para transmitir dicha instancia aleatoria a un usuario;

- medios (410) para generar, en dicho usuario, una respuesta por dicha función de respuesta en respuesta a dicha clave secreta y a dicha instancia aleatoria;

- medios para transmitir dicha respuesta de usuario a dicha parte intermediaria;

- medios (212) para generar, en dicha parte intermediaria, una respuesta de usuario enmascarada, por medio de la misma función de enmascaramiento que la de dicho centro de autentificación, en respuesta a dicha respuesta de usuario; y

- medios (214) para verificar, en dicha parte intermediaria, que dicha respuesta de usuario enmascarada se corresponde con dicha respuesta esperada enmascarada, con lo que autentifica al usuario.

19. El sistema de acuerdo con la reivindicación 18, **caracterizado por** medios adicionales para gestionar, en dicha parte intermediaria, información de prueba de autentificación que incluye al menos dicha respuesta de usuario recibida desde dicho usuario, e información de identificación de usuario correspondiente, con el fin de permitir que dicha parte intermediaria demuestre que dicho usuario ha sido autentificado.

20. El sistema de acuerdo con la reivindicación 19, **caracterizado por que** dicha información de prueba de autentificación incluye, adicionalmente, dicha instancia aleatoria.

21. El sistema de acuerdo con la reivindicación 18, **caracterizado por que** dichos medios para generar una respuesta esperada enmascarada y dichos medios para generar una respuesta de usuario enmascarada operan basándose en una instancia aleatoria de enmascaramiento común, para una seguridad incrementada.

22. El sistema de acuerdo con la reivindicación 19, **caracterizado por**:

- medios (240) para transmitir información de prueba de autentificación desde dicha parte intermediaria a dicho centro de autentificación; y

- medios (20) para verificar, en dicho centro de autentificación, si dicho usuario ha sido autentificado en dicha parte intermediaria basándose en dicha información de prueba recibida.

23. El sistema de acuerdo con la reivindicación 22, **caracterizado por que** dichos medios de verificación comprenden medios para comparar la repuesta de usuario de dicha información de prueba recibida con una respuesta esperada correspondiente proporcionada por dicho centro de autentificación.

24. El sistema de acuerdo con la reivindicación 23, **caracterizado por que** dicha información de prueba de autentificación incluye, adicionalmente, dicha instancia aleatoria, y dicho sistema comprende, adicionalmente, medios para recuperar, en dicho centro de autentificación, dicha clave secreta basándose en dicha identificación de usuario, y medios para volver a computar, en dicho centro de autentificación, dicha respuesta esperada a partir de dicha clave secreta recuperada y dicha instancia aleatoria.

25. El sistema de acuerdo con la reivindicación 19, **caracterizado por** medios adicionales para asociar a dicha parte intermediaria datos de autentificación generados para un usuario dado por dicho centro de autentificación con el fin de vincular información de prueba correspondiente con dicha parte intermediaria.

26. El sistema de acuerdo con la reivindicación 18, **caracterizado por**:

- medios para encriptar o cifrar datos transmitidos desde dicho centro de autentificación a dicha parte intermediaria por medio de dicha respuesta esperada; y

- medios para desencriptar o descifrar dichos datos cifrados en dicha parte intermediaria por medio de dicha respuesta de usuario recibida.

27. Un centro de autentificación para ayudar a la identificación de un usuario asociado en una parte intermediaria, capaz de llevar a cabo un procedimiento de respuesta ante instancia con el usuario, de tal modo que dicho centro de autentificación está **caracterizado por**:

- medios (14) para generar una respuesta esperada al menos parcialmente por la aplicación de una función de respuesta sobre una clave secreta, compartida con dicho usuario, y una instancia aleatoria;

- medios (16) para enmascarar dicha respuesta esperada por medio de una función de enmascaramiento con el fin de generar una respuesta esperada enmascarada; y

- medios (40) para transmitir dicha instancia aleatoria y dicha respuesta esperada enmascarada en respuesta a dicha parte intermediaria, que es, tras ello, capaz de autentificar al usuario en respuesta a una verificación positiva de que una respuesta de usuario enmascarada resultante corresponde a dicha respuesta esperada enmascarada.

28. El centro de autentificación de acuerdo con la reivindicación 27, **caracterizado por que** dichos medios de enmascaramiento son susceptibles de hacerse funcionar para enmascarar dicha respuesta esperada basándose en una instancia aleatoria de enmascaramiento común, para una seguridad incrementada.

29. El centro de autentificación de acuerdo con la reivindicación 27, **caracterizado por** medios adicionales para proteger criptográficamente datos transmitidos desde dicho centro de autentificación a dicha parte intermediaria por medio de dicha respuesta esperada.

30. El centro de autentificación de acuerdo con la reivindicación 27, **caracterizado por**:

- medios (30) para interrelacionar datos de autentificación generados para un usuario dado con información de identificación que identifica dicha parte intermediaria; y

- medios (20) para comparar dichos datos de autentificación con una representación de información de prueba recibida desde dicha parte intermediaria con el fin de verificar que dicha información de prueba está asociada con dicha parte intermediaria.

31. El centro de autentificación de acuerdo con la reivindicación 27, **caracterizado por que** dicho centro de autentificación es un corredor (750) que actúa como un centro de autentificación general o centro de identidad.

32. Un nodo (260) de red de parte intermediaria, gestionado por un proveedor de servicios e interconectado con un centro de autentificación (50, 150, 550) para autentificar a un usuario, asociado con el centro de autentificación, de acuerdo con un procedimiento de respuesta ante instancia, estando dicho nodo de red de parte intermediaria **caracterizado por**:

- medios (240) para recibir de dicho centro de autentificación una instancia aleatoria y una repuesta

esperada generada por una función de respuesta (14) a partir de una clave secreta, compartida con el usuario, y la instancia aleatoria, y a continuación enmascarada por una función de enmascaramiento;

- medios para transmitir la instancia aleatoria al usuario;

- medios para recibir de dicho usuario una respuesta de usuario también generada por dicha función de respuesta en respuesta a dicha clave secreta y dicha instancia intermedia, correspondiente a dicha respuesta esperada;

- medios (212) para generar una respuesta de usuario enmascarada por dicha función de enmascaramiento; y

- medios (214) para autentificar al usuario en respuesta a un resultado positivo de la verificación de que dicha respuesta de usuario enmascarada se corresponde con dicha respuesta esperada enmascarada.

33. El nodo de red de acuerdo con la reivindicación 32, **caracterizado por** medios adicionales para gestionar, en dicha parte intermediaria, información de prueba de autentificación, incluyendo al menos dicha respuesta de usuario recibida desde dicho usuario e información de identificación de usuario correspondiente, a fin de permitir a dicha parte intermedia demostrar que dicho usuario ha sido autentificado.

34. El nodo de red de acuerdo con la reivindicación 33, **caracterizado por que** dicha información de prueba de autentificación incluye, adicionalmente, dicha instancia aleatoria con el fin de ayudar a demostrar que dicho usuario ha sido autentificado por dicha parte intermediaria.

35. El nodo de red de acuerdo con la reivindicación 32, **caracterizado por que** dichos medios de generación son susceptibles de hacerse funcionar para generar dicha repuesta de usuario enmascarada basándose en una instancia aleatoria de enmascaramiento, de tal modo que dicha instancia aleatoria de enmascaramiento también es utilizada por dicho centro de autentificación para enmascarar dicha respuesta esperada.

36. El nodo de red de acuerdo con la reivindicación 32, **caracterizado por** medios adicionales para transmitir información de prueba desde dicha parte intermedia a dicho centro de autentificación.

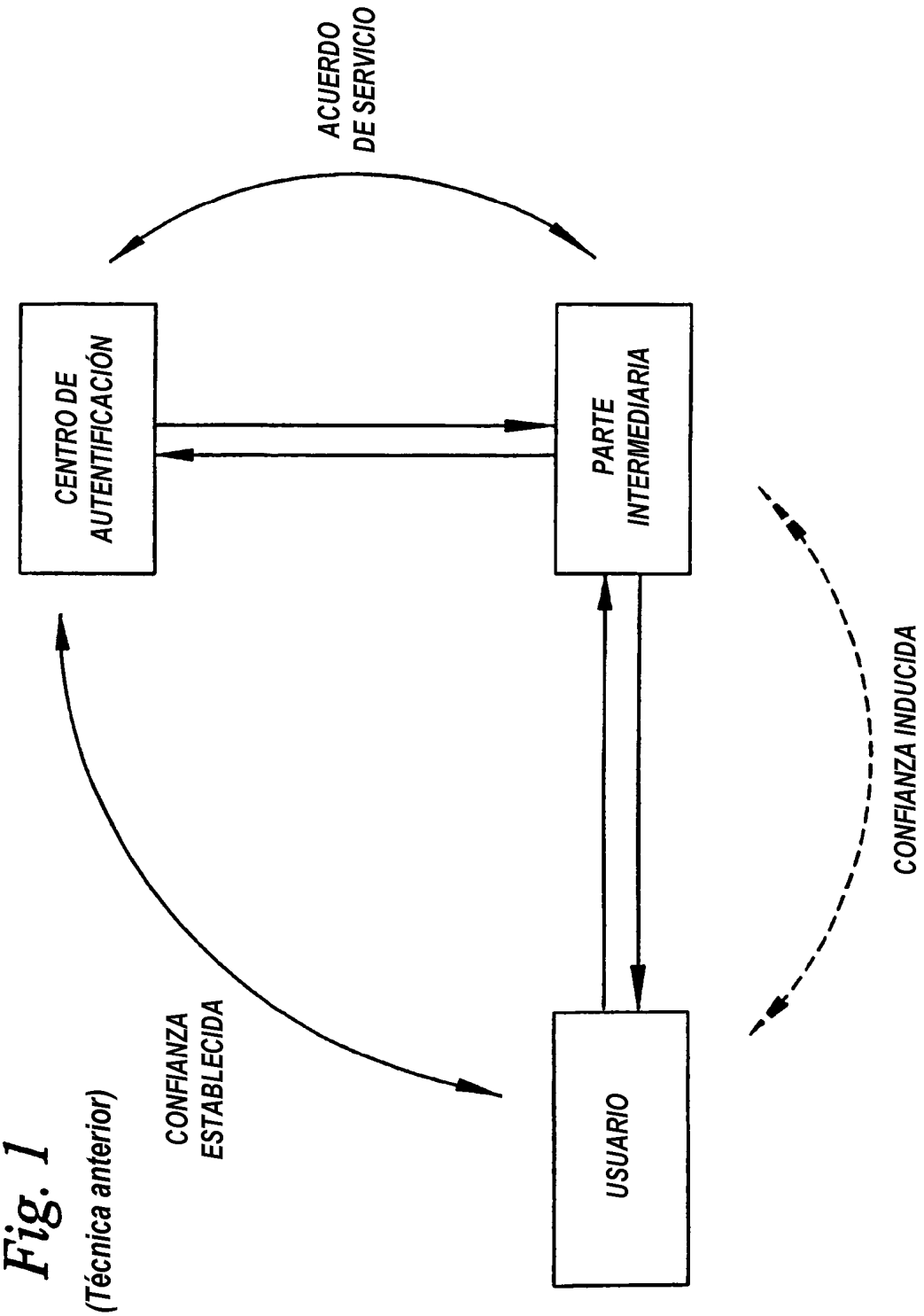
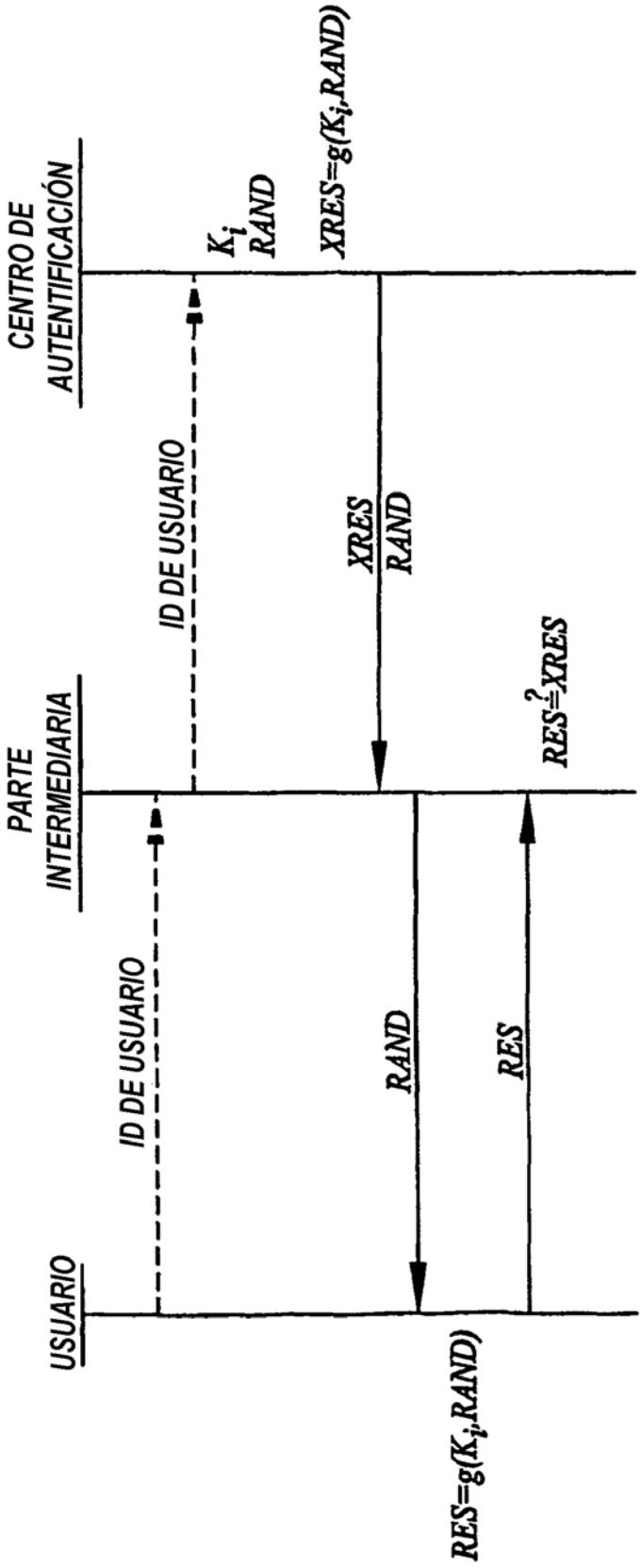


Fig. 1
(Técnica anterior)



(Técnica anterior)

Fig. 2

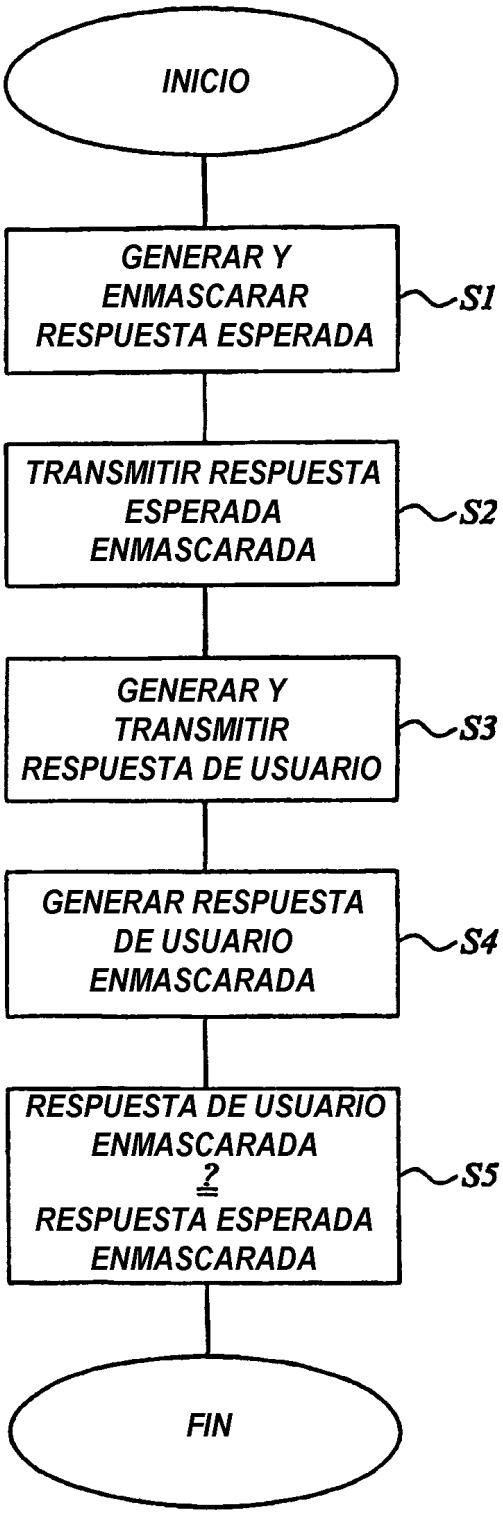

INICIO
GENERAR Y ENMASCARAR RESPUESTA ESPERADA
S1
TRANSMITIR RESPUESTA ESPERADA ENMASCARADA
S2
GENERAR Y TRANSMITIR RESPUESTA DE USUARIO
S3
GENERAR RESPUESTA DE USUARIO ENMASCARADA
S4
RESPUESTA DE USUARIO ENMASCARADA
≟
RESPUESTA ESPERADA ENMASCARADA
S5
FIN

Fig. 3

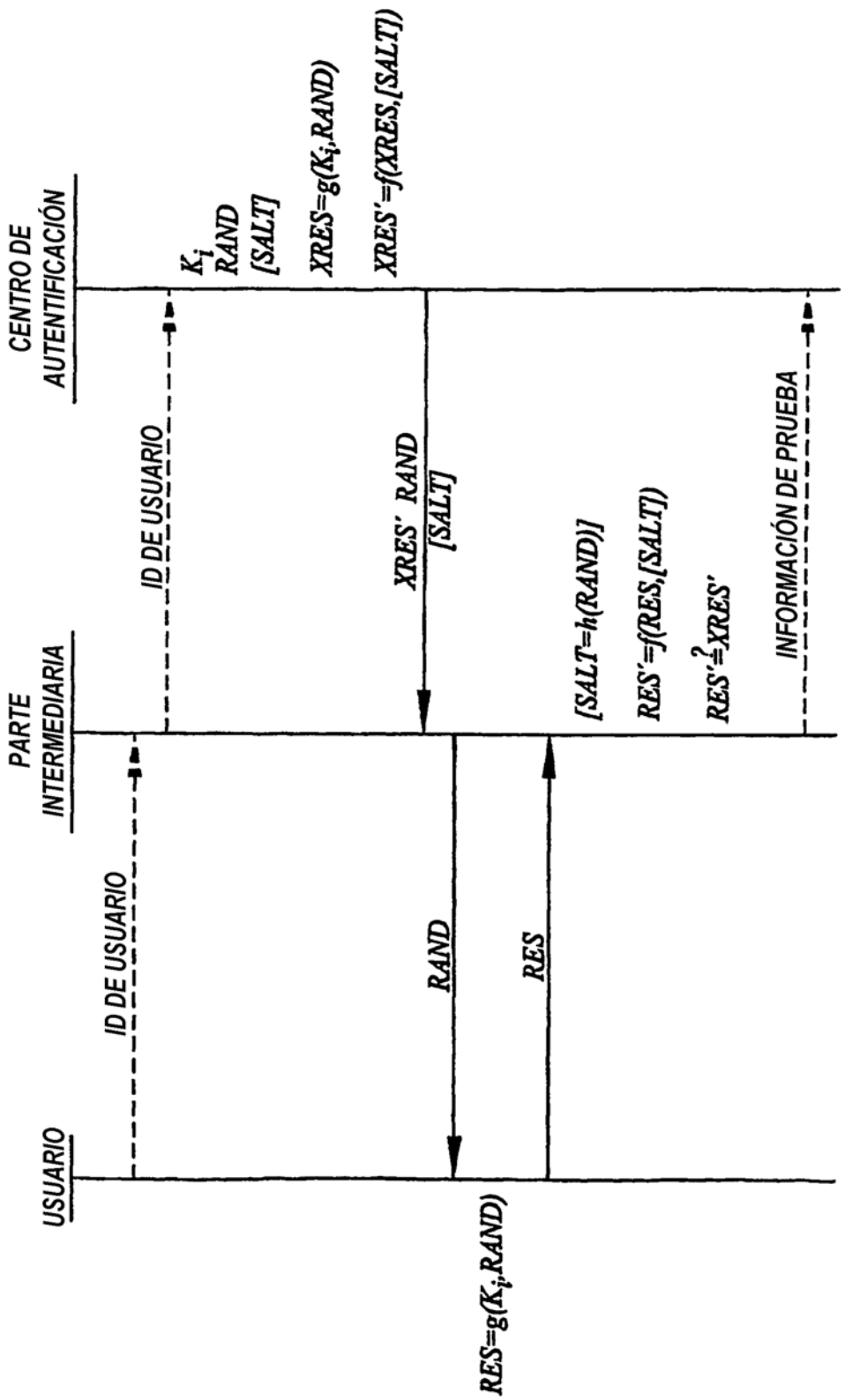

CENTRO DE AUTENTIFICACIÓN
PARTE INTERMEDIARIA
USUARIO
K_i
RAND
[SALT]
XRES=g(K_i,RAND)
XRES'=f(XRES,[SALT])
ID DE USUARIO
ID DE USUARIO
XRES' RAND
[SALT]
[SALT=h(RAND)]
RES'=f(RES,[SALT])
RES'$\stackrel{?}{=}$XRES'
INFORMACIÓN DE PRUEBA
RAND
RES
RES=g(K_i,RAND)

Fig. 4

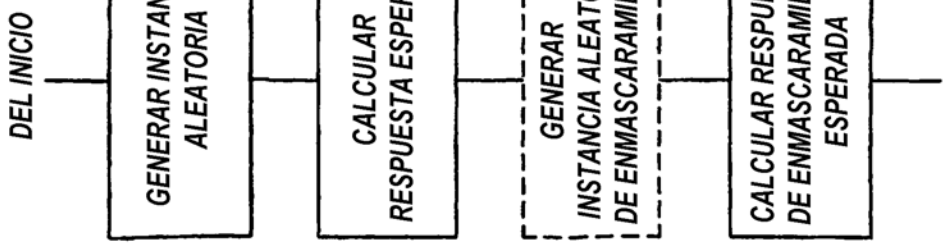

DEL INICIO
GENERAR INSTANCIA ALEATORIA
S11
CALCULAR RESPUESTA ESPERADA
S12
GENERAR INSTANCIA ALEATORIA DE ENMASCARAMIENTO
S13
CALCULAR RESPUESTA DE ENMASCARAMIENTO ESPERADA
S14

Fig. 5A

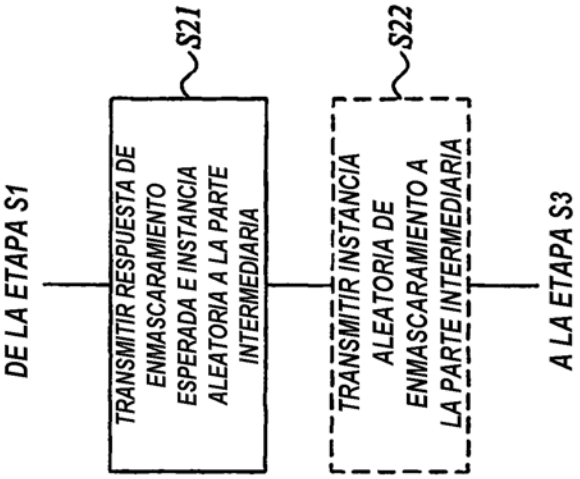

DE LA ETAPA S1
TRANSMITIR RESPUESTA DE ENMASCARAMIENTO ESPERADA E INSTANCIA ALEATORIA A LA PARTE INTERMEDIARIA
S21
TRANSMITIR INSTANCIA ALEATORIA DE ENMASCARAMIENTO A LA PARTE INTERMEDIARIA
S22
A LA ETAPA S3

Fig. 5B

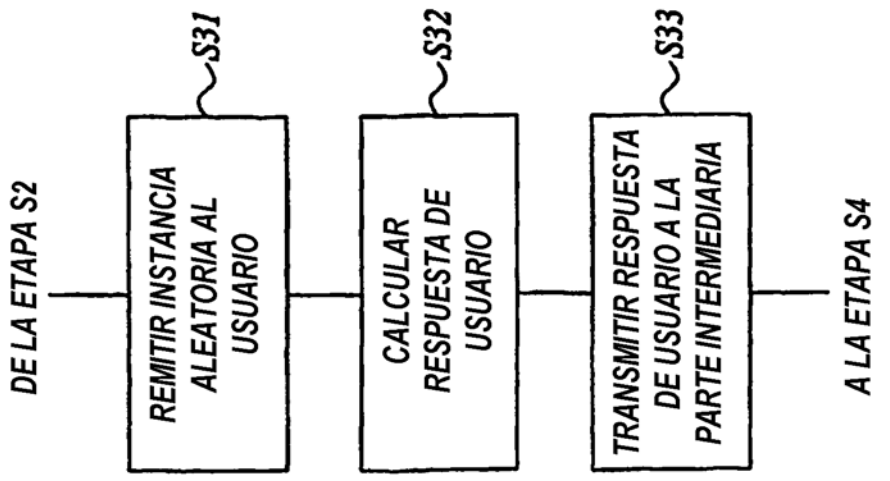


Fig. 5C

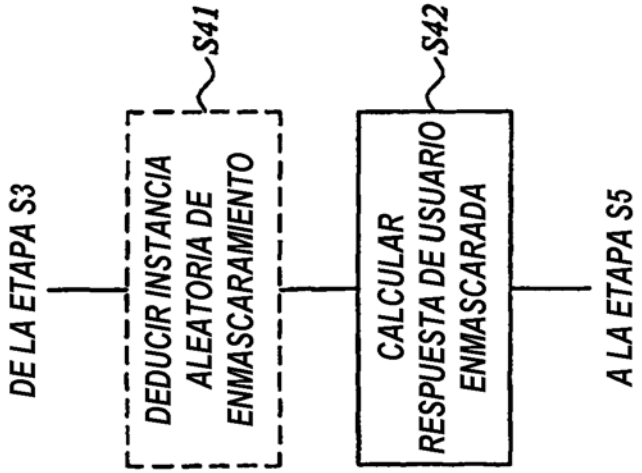


Fig. 5D

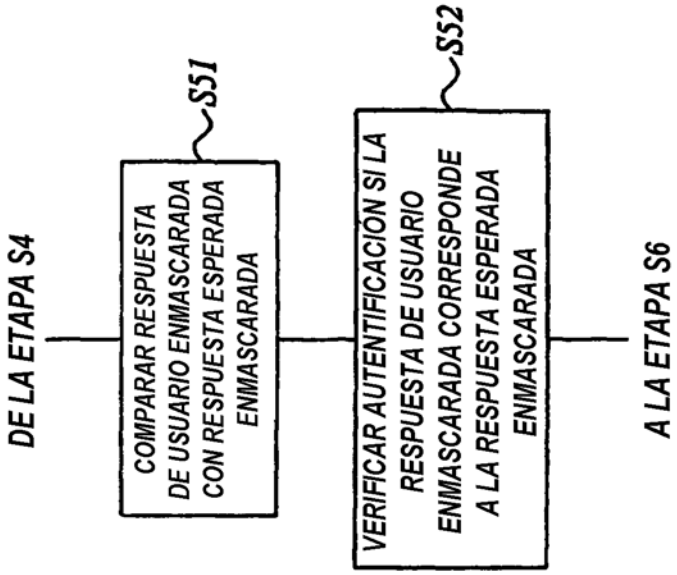


Fig. 5E

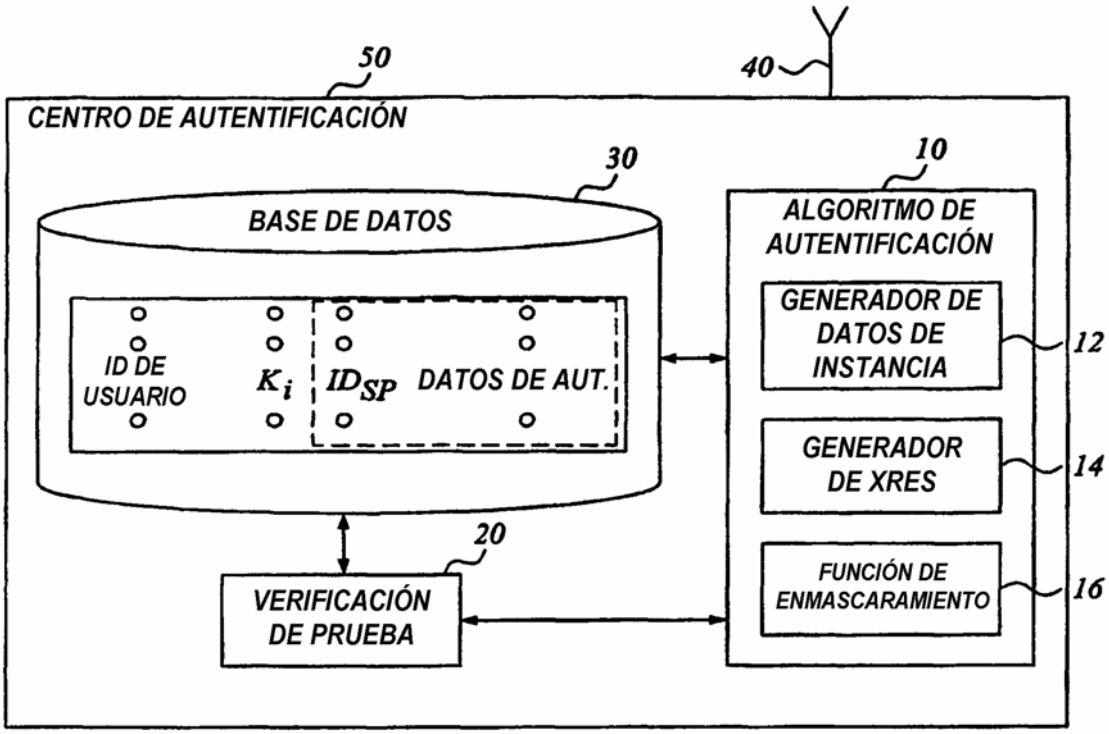

50
40
CENTRO DE AUTENTIFICACIÓN
30
10
BASE DE DATOS
ALGORITMO DE AUTENTIFICACIÓN
ID DE USUARIO
K_i
ID_{SP}
DATOS DE AUT.
GENERADOR DE DATOS DE INSTANCIA
12
GENERADOR DE XRES
14
20
FUNCIÓN DE ENMASCARAMIENTO
16
VERIFICACIÓN DE PRUEBA

Fig. 6

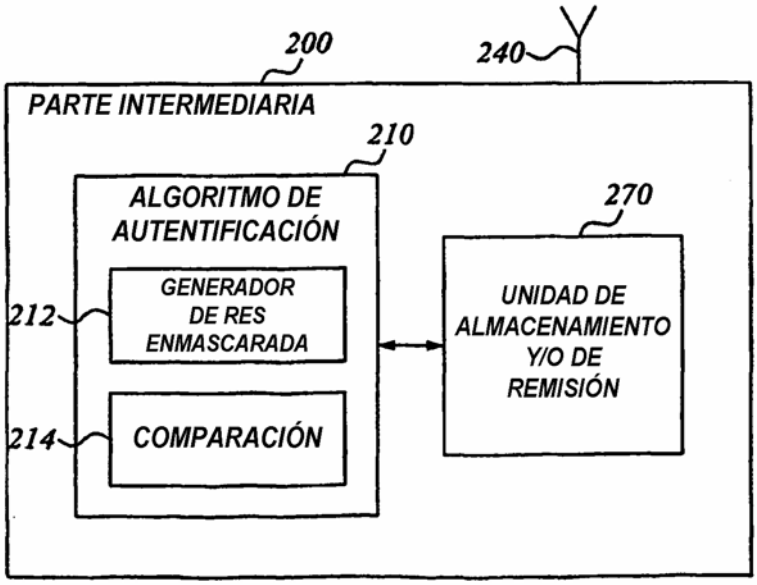
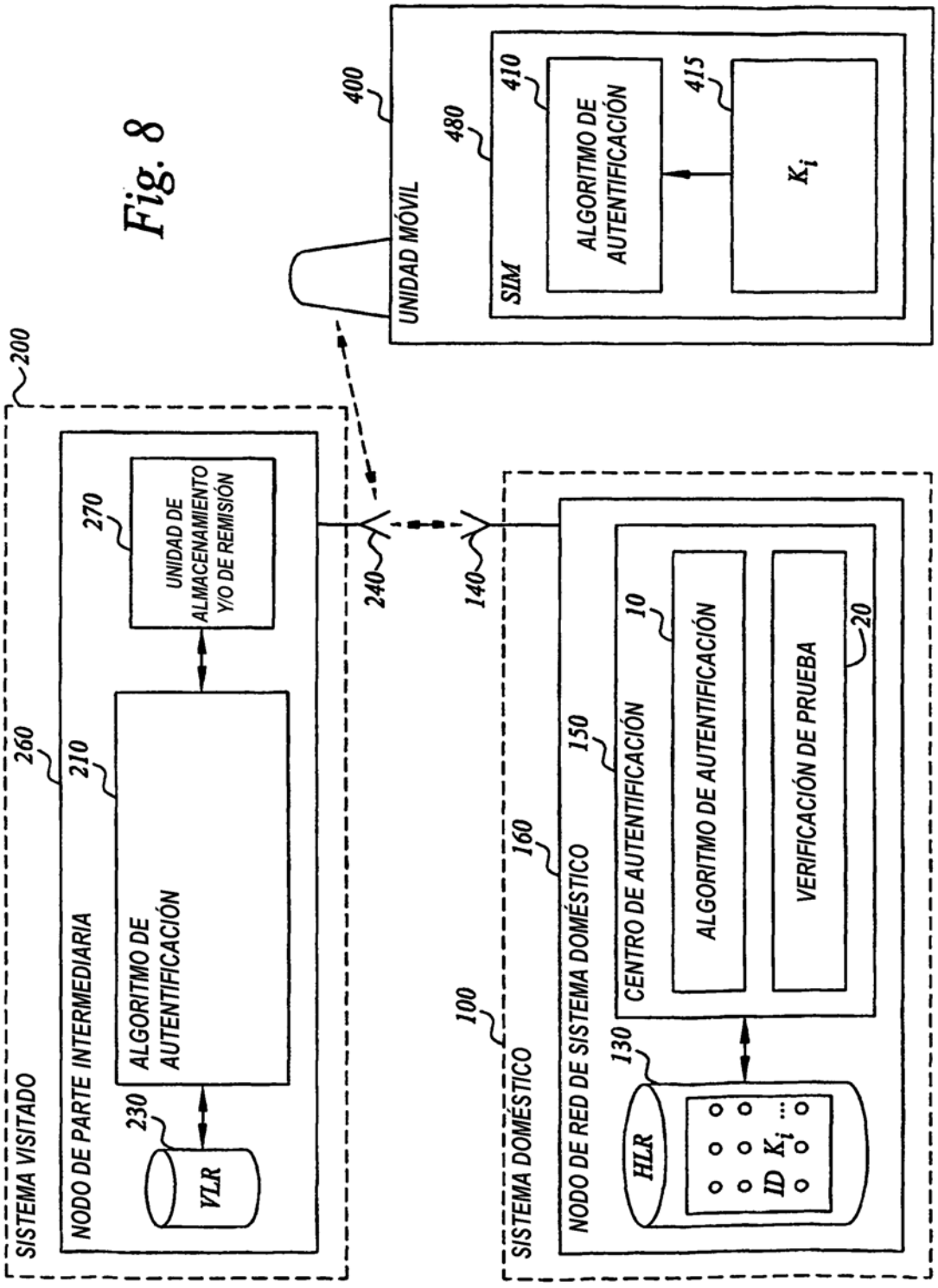

200
240
PARTE INTERMEDIARIA
210
ALGORITMO DE AUTENTIFICACIÓN
270
212
GENERADOR DE RES ENMASCARADA
UNIDAD DE ALMACENAMIENTO Y/O DE REMISIÓN
214
COMPARACIÓN

Fig. 7

Fig. 8


400
UNIDAD MÓVIL
480
SIM
410
ALGORITMO DE AUTENTIFICACIÓN
415
K_i
200
SISTEMA VISITADO
260
NODO DE PARTE INTERMEDIARIA
210
ALGORITMO DE AUTENTIFICACIÓN
270
UNIDAD DE ALMACENAMIENTO Y/O DE REMISIÓN
230
VLR
240
140
100
SISTEMA DOMÉSTICO
160
NODO DE RED DE SISTEMA DOMÉSTICO
150
CENTRO DE AUTENTIFICACIÓN
10
ALGORITMO DE AUTENTIFICACIÓN
20
VERIFICACIÓN DE PRUEBA
130
HLR
ID K_i ...

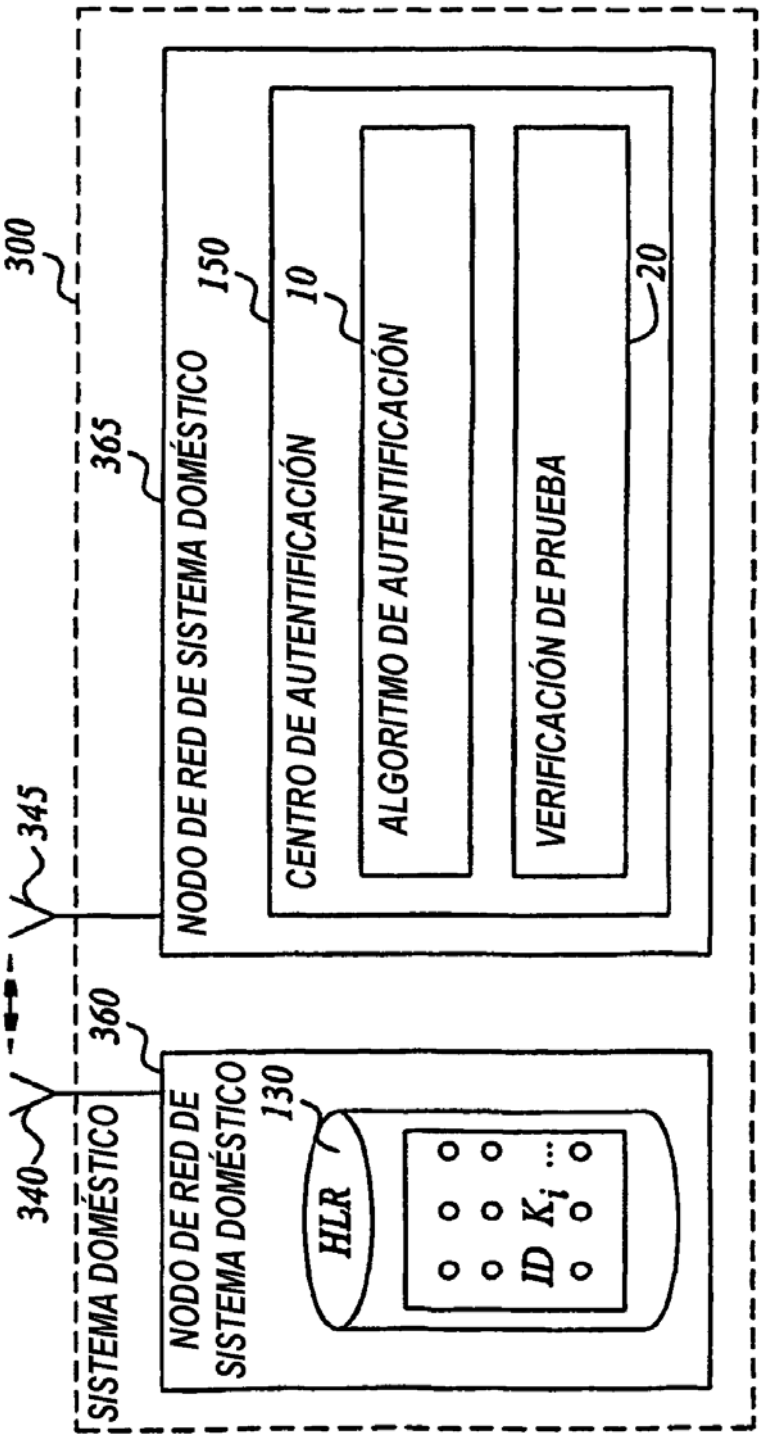

300
SISTEMA DOMÉSTICO
340
345
NODO DE RED DE SISTEMA DOMÉSTICO
360
130
HLR
ID K_i ...
NODO DE RED DE SISTEMA DOMÉSTICO
365
150
CENTRO DE AUTENTIFICACIÓN
10
ALGORITMO DE AUTENTIFICACIÓN
VERIFICACIÓN DE PRUEBA
20

Fig. 9

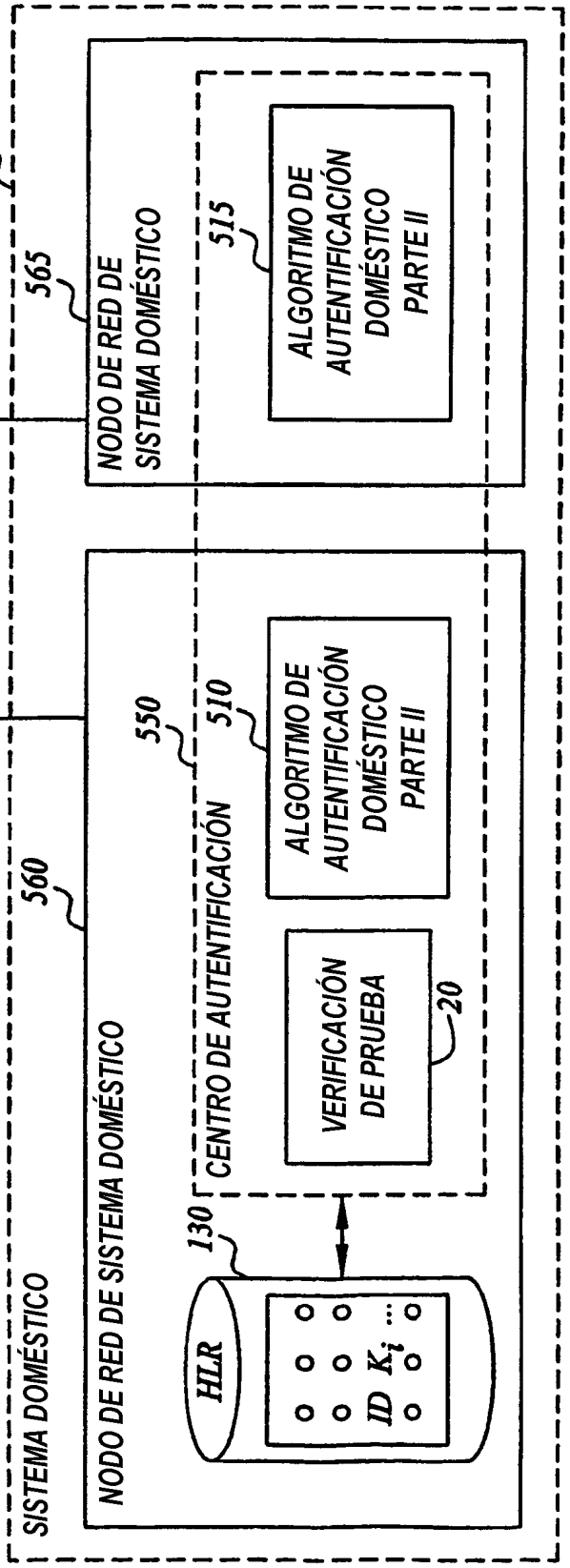

500
SISTEMA DOMÉSTICO
NODO DE RED DE SISTEMA DOMÉSTICO
560
540
550
CENTRO DE AUTENTIFICACIÓN
510
ALGORITMO DE AUTENTIFICACIÓN DOMÉSTICO PARTE II
VERIFICACIÓN DE PRUEBA
20
130
HLR
ID K_i ...
545
NODO DE RED DE SISTEMA DOMÉSTICO
565
515
ALGORITMO DE AUTENTIFICACIÓN DOMÉSTICO PARTE II

Fig. 10

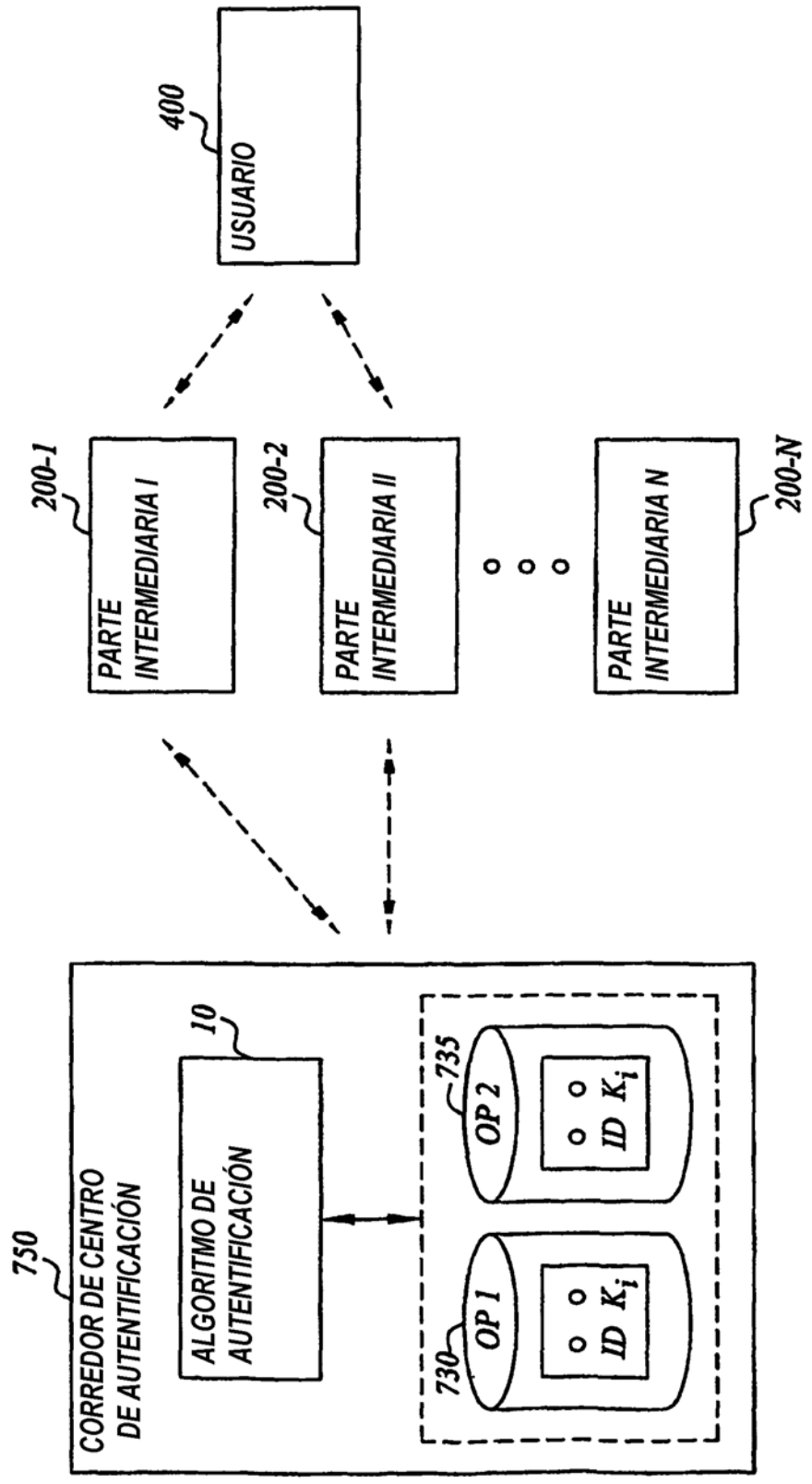

400
USUARIO
200-1
PARTE INTERMEDIARIA I
200-2
PARTE INTERMEDIARIA II
PARTE INTERMEDIARIA N
200-N
750
CORREDOR DE CENTRO DE AUTENTIFICACIÓN
10
ALGORITMO DE AUTENTIFICACIÓN
735
OP 2
ID K_i
730
OP 1
ID K_i

Fig. 11