(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 462 941**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.03.2008 E 08153102 (2)**

(97) Fecha y número de publicación de la concesión europea: **12.02.2014 EP 2104307**

(54) Título: **Transmisión segura de información específica de usuario en un servidor de red personal**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.05.2014

(73) Titular/es:

VODAFONE HOLDING GMBH (100.0%)
MANNESMANNUFER 2
40213 DÜSSELDORF, DE

(72) Inventor/es:

YANG, LU;
WILD, PETER y
DAWES, PETER

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Transmisión segura de información específica de usuario en un servidor de red personal

Campo técnico de la invención

La presente invención se refiere a un método para transmitir información específica de usuario confidencial entre un servidor de abonado doméstico y un servidor de gestión de red personal de una red personal en un dominio IMS de una red móvil, información que contiene una identidad de usuario privada de una estación móvil usada para un registro de estación móvil que utiliza la red personal.

Adicionalmente la presente invención se refiere a un sistema correspondiente para transmitir información específica de usuario confidencial entre un servidor de abonado doméstico y un servidor de gestión de red personal de una red personal en un dominio IMS de una red móvil, información que contiene una identidad de usuario privada de una estación móvil usada para un registro de estación móvil que utiliza la red personal.

Técnica anterior de la invención

Una red móvil de tercera generación, por ejemplo una red móvil de acuerdo con la norma UMTS (Sistema Universal de Telecomunicaciones Móviles), comprende un subsistema de conmutación de circuitos (CS) para conexiones de conmutación de circuitos, un subsistema de conmutación de paquetes (PS) que transmite paquetes de datos y un Subsistema Multimedia de Protocolo de Internet (IMS). En el UMTS estos subsistemas o áreas se denominan también como dominios y se proporcionan mediante la red central (dominio de red central) de la red móvil.

El dominio IMS proporciona servicios multimedia basados en IP (Protocolo de Internet). En particular el dominio IMS proporciona acceso a servicios de internet como telefonía por internet, radio por internet y televisión por internet para abonados móviles. Con el IMS se crea una plataforma combinada para servicios en tiempo real y otros servicios y se introduce una convergencia de elementos de red CS y PS. Pueden establecerse rápida y fácilmente nuevos servicios en el IMS usando servidores de aplicación. El dominio IMS tiene acceso a un Servidor de Abonado Doméstico (HSS) comprendido mediante la red móvil. El HSS mantiene perfiles de usuario y perfiles de servicio y es responsable de autenticación de usuario y autorización de acceso en la red móvil o para servicios proporcionados mediante la red móvil. El IMS es una arquitectura de red normalizada internacional para redes de telecomunicación de acuerdo con el 3GPP (Proyecto Común de la Tercera Generación) y es conocido por los expertos en la materia, por ejemplo a partir de la memoria descriptiva “3GPP TS 23.228 V8.2.0: IP multimedia subsystem; Etapa 2 (2007-09)”.

Para utilización de servicios mediante el IMS un abonado móvil se abona a un proveedor y obtiene una identidad de usuario privada (IMPI = Identificador de Usuario Privado Multimedia IP) y una o más identidades de usuario públicas (IMPU = Identificador de Usuario Público Multimedia IP). Con la identidad de usuario privada el abonado se registra en el domino IMS para utilización de servicios mediante el dominio IMS. Normalmente, una identidad de usuario privada se asigna a una tarjeta SIM (Módulo de Identificación de Abonado) y por lo tanto a una estación móvil que usa la tarjeta SIM. Por ejemplo una identidad de usuario privada puede contener un IMSI (Identificación Internacional de Abonado de Móvil) de 15 dígitos. Las identidades de usuario públicas se usan mediante cualquier abonado para solicitar comunicaciones a otros abonados. Por ejemplo se proporcionan las direcciones como direcciones SIP (Protocolo de Iniciación de Sesión). Las identidades de usuario públicas se describen en la sección 4.3.3.1 de la memoria descriptiva del 3GPP TS 23.228 V8.2.0.

Hoy en día más y más abonados móviles poseen dos o más estaciones móviles con diferentes capacidades y un número creciente de dispositivos en el área privada de un abonado móvil tales como aparatos domésticos, sistemas de alarma y unidades de vídeo y audio proporcionan interfaces que posibilitan una conexión a una estación móvil o a una red doméstica. Por lo tanto, se proporcionan las denominadas redes privadas o personales (PN) con un dispositivo de gestión (PNM: Gestión de Red Personal) en una red móvil para facilitar la aplicación y administración de las diferentes estaciones móviles y dispositivos compatibles con red para un usuario.

Por medio de la PNM se establece y se gestiona una interconexión de red con todas las estaciones móviles y dispositivos con capacidad de red que pertenecen a un usuario usando las conexiones convencionales proporcionadas mediante la red móvil. Una configuración de la PNM puede conseguirse mediante el usuario o mediante un operador de la red móvil. Por ejemplo una red personal posibilita un reenvío de mensajes recibidos a la estación móvil más adecuada con respecto al formato de datos del mensaje y/o con respecto a los ajustes PN de los usuarios. Se conocen las redes personales por los expertos en la materia y se especifican, por ejemplo, en las memorias descriptivas “3GPP TS 22.259 V8.3.0: Service requirements for Personal Network Management (PNM); Etapa 1 (2006-06)” y “3GPP TS 23.259 V1.2.0: Personal Network Management (PNM), Procedures and Information Flows; Etapa 2 (2007-11)”.

En la memoria descriptiva “3GPP TS 23.259 V1.2.0: Personal Network Management (PNM), Procedures and Information Flows; Etapa 2 (2007-11)” se describe una transmisión de una identidad de usuario privada desde un

servidor de abonado doméstico a un servidor de gestión de red personal durante un registro de una estación móvil en una red personal.

La memoria descriptiva “ETSI TS 133 220 V7.10.0: Digital cellular telecommunications system (Fase 2+); UMTS; Generic Authentication Architecture (GAA); Generic bootstrapping architecture (2007-11)” describe características de seguridad y un mecanismo para autenticación de arranque y acuerdo de clave para seguridad de aplicación en un entorno 3GPP.

Mientras que un usuario registra una estación móvil en una red personal utilizando la red personal normalmente se solicita información específica de usuario confidencial desde un servidor de abonado doméstico en la red móvil y se transmite desde el servidor de abonado doméstico a la PNM mediante la red móvil y redes asociadas como internet, opcionalmente. En la PNM la información específica de usuario confidencial se usa para autenticación y autorización de usuario. Al hacer esto tiene la desventaja de que la información específica de usuario confidencial tal como una identidad de usuario privada se transmite a la PNM en texto en claro. Esto conduce a un riesgo de seguridad significativo, debido a que una persona no autorizada puede obtener información específica de usuario confidencial y usar indebidamente esta información.

Divulgación de la invención

El objetivo de la presente invención es satisfacer la desventaja anteriormente descrita y proporcionar una transmisión segura y fiable de información específica de usuario confidencial desde un servidor de abonado doméstico a un servidor de gestión de una red personal durante un registro de una estación móvil en la red personal.

De acuerdo con la presente invención el objetivo se consigue en que un método como se describe en el comienzo de transmitir información específica de usuario confidencial entre un servidor de abonado doméstico y un servidor de gestión de red personal de una red personal en un dominio IMS de una red móvil, información que contiene una identidad de usuario privada de una estación móvil usada para un registro de estación móvil que utiliza la red personal, comprende las etapas de

a) proporcionar una clave digital al servidor de abonado doméstico y al servidor de gestión de red personal usada para encriptar y desencriptar la identidad de usuario privada, siendo la clave digital un número aleatorio con la misma longitud de bits que la identidad de usuario privada;

b) encriptar la identidad de usuario privada en el servidor de abonado doméstico, en el que el formato de datos y la longitud de datos de la identidad de usuario privada encriptada corresponde al formato de datos y a la longitud de datos de la identidad de usuario privada no encriptada;

c) transmitir una solicitud de registro que incluye la identidad de usuario privada y una identidad de usuario pública desde la estación móvil a una unidad de registro en una unidad de control de sesión de llamada del dominio IMS que solicita registro en la red personal;

d) recibir la solicitud de registro desde la estación móvil en la unidad de registro en la unidad de control de sesión de llamada de la red móvil que solicita un registro en la red personal;

e) interrogar al servidor de abonado doméstico mediante la unidad de control de sesión de llamada del dominio IMS para información específica de usuario que contiene la identidad de usuario privada encriptada y una dirección y/o nombre del servidor de gestión de red personal;

f) transmitir la identidad de usuario privada encriptada desde el servidor de abonado doméstico al servidor de gestión de red personal mediante la unidad de control de sesión de llamada, en el que la identidad de usuario privada encriptada recibida desde el servidor de abonado doméstico y la identidad de usuario pública recibida desde la estación móvil se reenvían desde la unidad de control de sesión de llamada al servidor de gestión de red personal en una solicitud de registro de terceros;

g) desencriptar la identidad de usuario privada encriptada recibida en el servidor de gestión de red personal;

h) registro de la estación móvil en la red personal mediante el servidor de gestión de red personal usando la identidad de usuario privada desencriptada y la identidad de usuario pública.

Adicionalmente, el objetivo se consigue con un sistema correspondiente de acuerdo con la reivindicación 5.

El principio básico de la presente invención es proporcionar información específica de usuario confidencial encriptada en el servidor de abonado doméstico y transmitir la información específica de usuario confidencial encriptada al servidor de gestión de red personal para un registro de una estación móvil en la red personal. Al hacer esto la información específica de usuario confidencial siempre se pasa al servidor de gestión de red personal encriptada y oculta respectivamente.

La información específica de usuario confidencial comprende una identidad de usuario privada de la estación móvil. La identidad de usuario privada está diseñada para autenticación y autorización de una estación móvil y un usuario respectivamente para el dominio IMS de una red móvil. Por lo tanto la identidad de usuario privada es particularmente adecuada para una autenticación y autorización durante el registro en una red personal. Adicionalmente algunos servicios proporcionados mediante la red personal requieren la identidad de usuario privada. Transmitiendo la identidad de usuario privada encriptada al servidor de gestión de red personal se aumenta la seguridad y la fiabilidad del uso de los servicios de red personal.

El formato de datos y la longitud de datos de la identidad de usuario privada encriptada corresponden al formato de datos y a la longitud de datos de la identidad de usuario privada no encriptada. Como resultado la identidad de usuario privada se oculta en la identidad de usuario privada encriptada, que tiene la apariencia de una identidad de usuario privada normal no encriptada. Por lo tanto, la identidad de usuario privada encriptada se puede transmitir con todas las corrientes de datos, dispositivos de transmisión y métodos que comprenden una identidad de usuario privada sin cambios costosos y molestos.

El método de acuerdo con la presente invención está basado en lo mismo, que se proporciona una clave digital al servidor de abonado doméstico y al servidor de gestión de red personal usada para encriptar y desencriptar la información específica de usuario confidencial. La clave digital se usa mediante un módulo de encriptación que genera información específica de usuario confidencial encriptada y mediante un módulo de desencriptación que decodifica la información específica de usuario encriptada. Al hacer esto, puede conseguirse una encriptación simétrica o una asimétrica. Usando un módulo de encriptación junto con una clave digital se obtiene una encriptación muy segura. Adicionalmente, pueden usarse diferentes claves digitales para diferentes usuarios o para un usuario sucesivamente con el mismo módulo de encriptación y módulo de desencriptación. Esto reduce significativamente el esfuerzo de instalación y permite variar la encriptación de una manera fácil.

En el dispositivo de acuerdo con la presente invención se proporciona un generador de clave en la red móvil que proporciona una clave digital al servidor de abonado doméstico y al servidor de gestión de red personal para encriptar y desencriptar información específica de usuario confidencial. Al igual que en el método correspondiente se usa la clave digital mediante el módulo de encriptación y el módulo de desencriptación para encriptar y desencriptar la información específica de usuario simétrica o asimétricamente. Por lo tanto se obtiene una encriptación segura con diferentes claves digitales para diferentes usuarios o para un usuario sucesivamente usando el mismo módulo de encriptación y desencriptación. Se reduce significativamente el esfuerzo de instalación y mantenimiento y la encriptación es fácilmente personalizable para diferentes usuarios.

Por ejemplo, la unidad de control de sesión de llamada puede realizarse mediante un servidor S-CSCF (Función de Control de Sesión de Llamada - de Servicio) en el dominio IMS. Como se conoce bien en la técnica un servidor S-CSCF es responsable del registro de usuarios, gestión de estado de sesión e interacción con plataformas de servicio en el dominio IMS. Con las etapas anteriormente mencionadas se consigue un reenvío de una identidad de usuario privada encriptada y una identidad de usuario pública al servidor de gestión de red personal durante un registro de una estación móvil en la red personal de una manera segura y eficaz.

Por lo tanto el método y el dispositivo correspondiente de acuerdo con la presente invención eliminan los problemas de privacidad producidos al transmitir información específica de usuario confidencial en texto en claro usando una interfaz insegura entre el servidor de abonado doméstico y el servidor de gestión de red personal. Un usuario puede registrar su estación móvil en una red personal de una manera segura sin el riesgo de revelar información confidencial. Por lo tanto se evita eficazmente un uso fraudulento de información específica de usuario confidencial.

Preferentemente, la clave digital tiene un periodo de validez limitado en una realización del método para transmitir información específica de usuario confidencial de acuerdo con la presente invención. Por ejemplo el periodo de validez puede limitarse a la duración de un registro o a una cierta cantidad de días, semanas o meses. Al hacer esto se aumenta sustancialmente la seguridad de la encriptación, debido a que se evitan intentos no autorizados de encriptar información específica de usuario confidencial con cada renovación de la clave digital. Otra realización ventajosa del método para transmitir información específica de usuario confidencial de acuerdo con la presente invención comprende las etapas de

a) transmitir la identidad de usuario privada encriptada recibida desde el servidor de gestión de red personal al servidor de abonado doméstico;

b) transmitir al menos una identidad de usuario pública asignada a la identidad de usuario privada encriptada mediante el servidor de abonado doméstico desde el servidor de abonado doméstico al servidor de gestión de red personal; y

c) verificar la identidad de usuario pública recibida desde la unidad de control de sesión de llamada usando la identidad de usuario pública recibida desde el servidor de abonado doméstico mediante el servidor de gestión de red personal durante un registro de la estación móvil en la red personal.

Usando estas etapas se consigue una verificación muy eficaz de la identidad de usuario pública recibida desde la estación móvil mediante la unidad de control de sesión de llamada en el servidor de gestión de red personal. Por ejemplo el servidor de gestión de red personal puede verificar si la identidad de usuario pública recibida está enmascarada o no. Los identificadores enmascarados se usan a menudo en redes locales al igual que en redes domésticas. La identidad de usuario privada encriptada se devuelve al servidor de abonado doméstico mejorando la seguridad de datos durante la verificación. Por lo tanto, con esta realización se aumenta sustancialmente la fiabilidad de usar los servicios de red personal.

En una realización ventajosa adicional del método para transmitir información específica de usuario confidencial de acuerdo con la presente invención se usa una función XOR a nivel de bit para encriptación y desencriptación de la información específica de usuario confidencial. La función XOR a nivel de bit es una operación a nivel de bit muy común proporcionada mediante ordenadores y chips independientes. Por lo tanto se consigue una encriptación que usa una operación XOR a nivel de bit con datos a encriptar y una clave digital de una manera muy fácil y barata.

Resultan realizaciones y ventajas adicionales de la materia objeto de las reivindicaciones dependientes así como del dibujo con la descripción adjunta.

A continuación se describe un ejemplo no limitante de una realización de acuerdo con la presente invención en detalle con referencia al dibujo adjunto.

Breve descripción del dibujo

La Figura 1 muestra esquemáticamente una realización de un método y un dispositivo de la presente invención que transmite información específica de usuario confidencial entre un servidor de abonado doméstico y un servidor de gestión de red personal.

Descripción de una realización preferida

Con referencia de nuevo a la Figura 1 se muestra una red móvil y se designa mediante el número 1. Por ejemplo, la red móvil 10 es acorde con la norma GSM/GPRS, UMTS, CDMA2000, FOMA, TD-SCDMA o WiMAX o una norma de cuarta generación. Estas redes móviles con los elementos y funciones correspondientes son bien conocidas por los expertos en la materia. Para simplificar se muestra la red móvil 10 esquematizada como una nube en la Figura 1 que incluye un mástil de radio 12. La red móvil 10 comprende un dominio de Subsistema Multimedia de Protocolo de Internet (IMS) 14 que integra y proporciona servicios multimedia basados en IP y otros servicios para usuarios.

El dominio IMS 14 contiene una unidad de control de sesión de llamada 16para registro de usuario y estado de llamada y administración de estado de sesión del dominio IMS 14. En esta realización la unidad de control de sesión de llamada 16está implementada en un proxy SIP S-CSCF (servidor de Protocolo de Iniciación de Sesión de Función de Control de Sesión de Llamada - de Servicio). Por lo tanto a continuación la unidad de control de sesión de llamada 16se denomina como S-CSCF 16 por simplicidad. El S-CSCF 16 comprende una unidad de registro 18 para el registro de estaciones móviles en el dominio IMS 14. Adicionalmente la red móvil 10 comprende un Servidor de Abonado Doméstico (HSS) 20 accesible desde el dominio IMS 16. El HSS 20 mantiene perfiles de usuario y perfiles de servicio y es responsable de autenticación de usuario y autorización de acceso en la red móvil 10 o para servicios proporcionados mediante la red móvil 10. El S-CSCF 16 y el HSS 20 son componentes bien conocidos de una red móvil anteriormente descrita.

Más adelante se muestra un usuario 24 de la red móvil 10 en la Figura 1. El usuario 24 a modo de ejemplo tiene tres dispositivos 26, 28, 30 que pueden transmitir o recibir voz u otros datos a través de una red de telecomunicación o red de datos pública. Al menos el dispositivo 26 es una estación móvil 26. Por ejemplo, la estación móvil 26 puede ser un teléfono móvil, un teléfono de coche, un teléfono inteligente, un ordenador fijo (por ejemplo PC) o un ordenador móvil (por ejemplo portátil, PDA) u otro dispositivo con un módulo de interfaz de radio 32 integrado o enchufado (por ejemplo tarjeta PMCCIA), o un dispositivo conectado a una estación móvil mediante una interfaz y que usa la estación móvil para comunicación. La estación móvil 26 es con capacidad de IMS y posibilita a un usuario comunicarse mediante la red móvil 10 y usar servicios mediante el dominio IMS 14. Los otros dispositivos 28 y 30 pueden ser, por ejemplo, estaciones móviles, sistemas de telefonía fija u ordenadores conectados a una red de telecomunicación o internet.

Para utilización del dominio IMS 14 se proporciona la estación móvil 26 con una identidad de usuario privada 34 (IMPI: Identificador de Usuario Privado Multimedia IP). El IMPI 34 se usa para registro del dominio IMS 14 utilizando servicios de dominio IMS. Para ser alcanzable por otros usuarios o servicios a través del domino IMS 14 se proporciona al usuario 24 con una o más identidades de usuario públicas 36 (IMPU: ID de Usuario - Identificador Público Multimedia IP). El IMPU 36 representa una dirección de usuario pública y es independiente del dispositivo. El IMPI 34 y el IMPU 36 se proporcionan al HSS 20 y a la estación móvil 26 durante el aprovisionamiento de servicio IMS.

La estación móvil 26 y los otros dispositivos 28 y 30 tienen diferentes características y capacidades. Pueden también usarse en diferentes lugares como en el hogar, en una oficina o en la carretera. Para simplificar el uso, mantenimiento y coordinación de la estación móvil 26 y los otros dispositivos 28, 30 se establece una red personal 38 que comprende la estación móvil 26 y los otros dispositivos 28, 30 usando el dominio IMS 14. Para este fin se proporciona un servidor de gestión de red personal 40como un servidor de aplicación en el dominio IMS 14. A continuación el servidor de gestión de red personal 40se denomina también como PNM-AS 40 (Servidor de Aplicación - Gestión de Red Personal). El PNM-AS 40 establece y administra la red personal 38 y posibilita comunicación y reenvío de llamadas y sesiones entre la estación móvil 26 y los otros dispositivos 28, 30. Por ello se consigue la transmisión real de datos en la red personal 38 mediante conexiones convencionales proporcionadas mediante la red móvil 10 u otras redes de telecomunicación o redes de datos. El IMPI 34 de la estación móvil 26 se proporciona al PNM-AS 40 durante el aprovisionamiento de servicio de red personal. El PNM-AS 40 también comprende un dispositivo de registro 42 para el registro de las estaciones móviles en la red personal 38 utilizando servicios de red personal usando el IMPI 34 para autenticación y autorización. Se proporcionan servicios de gestión de red personal al usuario 24 mediante el PNM-AS 40.

Para una transmisión segura de información específica de usuario confidencial al igual que el IMPI 34 el HSS 20 comprende un módulo de encriptación 44 y el dispositivo transmisor 46 que transmite información específica de usuario confidencial encriptada al PNM-AS 40. El módulo de encriptación 44 encripta información específica de usuario usando una clave digital 48 denominada de manera ejemplar SPND 48 (Datos de Red Personal de Abonado). Los SPND 48 (clave digital) se generan mediante un generador de clave digital 50 proporcionado en la red móvil 10. Por ejemplo la clave digital 48 puede ser un número aleatorio con la misma longitud de bits que el IMPI 34 y se genera mediante un generador de números aleatorios comprendido en el generador de clave digital 50. La clave digital 48 puede tener un periodo de validez limitado controlado mediante un temporizador 52 en la red móvil 10.

La desencriptación de la información específica de usuario confidencial encriptada recibida en el PNM-AS 40 se hace mediante un módulo de desencriptación 54 comprendido mediante el PNM-AS 40.

A continuación se describe la funcionalidad de los dispositivos anteriormente mencionados y las etapas del método de acuerdo con la realización en detalle.

Para conseguir una transmisión segura del IPMI 34 desde el HSS 20 al PNM-AS 40 para un registro de la estación móvil 26 en la red personal 28 en primer lugar se generan unos SPND 48 (clave digital) mediante el generador de clave digital 50 y se proporciona al HSS 20 y al PNM-AS 40 por medio de aprovisionamiento de servicios de gestión de red personal, flechas 60. Los SPND 48 (clave digital) son un número aleatorio con la misma longitud de bits que el correspondiente IPMI 34 y se genera únicamente para todos los servicios de gestión de red personal o se genera individualmente para cada suscripción de un usuario de red personal 24.

Cuando el usuario 24 quiere usar los servicios de red personal proporcionados mediante el PNM-AS 40 con su estación móvil 26, envía (flecha 64) una solicitud de registro SIP 62 que contiene el IMPI 34 y el IMPU 36 desde la estación móvil 26 a la unidad de registro 18 en el S-CSCF 16. El S-CSCF 16 interroga al HSS 20 para información de usuario reenviando (flecha 66) al menos el IMPI 34 en una consulta al HSS 20, por ejemplo usando una interfaz Cx. Opcionalmente el IMPU 36 también se reenvía al HSS 20 en la consulta.

Al recibir la consulta el HSS 20 encripta inmediatamente el IMPI 34 o proporciona un IMPI 68 pre-encriptado usando el módulo de encriptación 44. El módulo de encriptación 44 encripta el IMPI 34 usando una función con el IMPI 34 y los SPND 48 (clave digital) como parámetros. Por lo tanto el IMPI 68 encriptado se denomina también como f(IMPI, SPND) 68 en la Figura 1. Por ejemplo la función puede ser un XOR a nivel de bit. Adicionalmente los bits del IMPI 34 pueden desplazarse antes de ejecutar la función. El HSS 20 a continuación transmite una respuesta a la consulta que contiene al menos el IMPI 68 encriptado (f(IMPI, SPND)) y una dirección 70 del PNM-AS 40, usando el dispositivo transmisor 46, flecha 72. Opcionalmente se incluye el IMPU 36 en la respuesta.

El S-CSCF 16 pasa el IMPI 68 encriptado (f(IMPI, SPND)) y el IMPU 36 al PNM-AS 40 en una solicitud de registro de terceros 73, flecha 74. En el PNM-AS 40 el IMPI 68 encriptado (f(IMPI, SPND)) se desencripta mediante el módulo de desencriptación 54 usando la función inversa de la función usada para encriptación con el IMPI 68 encriptado (f(IMPI, SPND)) y los SPND 48 (clave digital) como parámetros. Por lo tanto f'(f(IMPI, SPND), SPND) se refiere al IMPI 34 no encriptado en la Figura 1. Por ejemplo, si la función XOR a nivel de bit se usa para encriptación, la función XOR a nivel de bit se usa también para desencriptación, debido a que esta función es una función involutiva. Posteriormente el IMPU 36 y el IMPI 34 desencriptado se usan mediante el dispositivo de registro 42 en el PNM-AS 40 para registro de la estación móvil 26 en la red personal 38 utilizando servicios de red personal. De esta manera el IMPI 34 se usa para autenticación y autorización de la estación móvil 26 y el usuario 24 respectivamente.

Opcionalmente el PNM-AS 40 puede interrogar al HSS 20 para el IMPU 36 que está correlacionado con el IMPI 34 mediante el aprovisionamiento antes de registro de la estación móvil 26 en la red personal 38. Al hacer esto, el PNM-AS 40 envía el IMPI 68 (f(IMPI, SPND)) encriptado recibido al HSS 20, flecha 76. El HSS 20 devuelve el IMPU 36 correlacionado y otros IMPU correlacionados pre-configurados en el HSS 20 junto con el SPND 48 y el IMPI 34,

flecha 78. A continuación el PNM-AS 40 verifica si el IMPU 36 devuelto es idéntico al recibido desde el S-CSCF 16. Esta interrogación proporciona un método seguro para que el PNM-AS 40 verifique si el IMPU 36 recibido está enmascarado o no y por lo tanto aumenta la fiabilidad para usar los servicios de red personal.

Usando la realización descrita el IMPI 34 siempre se pasa a y se envía desde el PNM-AS 40 encriptado y oculto respectivamente. Por lo tanto la realización descrita supera los problemas de privacidad producidos al transmitir el IMPI 34 en texto en claro usando una interfaz insegura entre el S-CSCF 16 y el PNM-AS 40.

REIVINDICACIONES

1. Un método para transmitir información específica de usuario confidencial (34) entre un servidor de abonado doméstico (20) y un servidor de gestión de red personal (40) de una red personal (38) en un dominio IMS (14) de una red móvil (10), información (34) que contiene una identidad de usuario privada (34) de una estación móvil (26) usada por un registro de un estación móvil (26) que utiliza la red personal (38), comprendiendo el método las etapas de

a) proporcionar una clave digital (48) al servidor de abonado doméstico (20) y al servidor de gestión de red personal (40) usada para encriptar y desencriptar la identidad de usuario privada (34), siendo la clave digital (48) un número aleatorio con la misma longitud de bits que la identidad de usuario privada (34);
b) encriptar la identidad de usuario privada (34) en el servidor de abonado doméstico (20), en donde el formato de datos y la longitud de datos de la identidad de usuario privada (68) encriptada se corresponden con el formato de datos y la longitud de datos de la identidad de usuario privada (34) no encriptada;
c) transmitir (64) una solicitud de registro (62) que incluye la identidad de usuario privada (34) y una identidad de usuario pública (36) desde la estación móvil (26) a una unidad de registro (18) en una unidad de control de sesión de llamada (16) del dominio IMS (14) que solicita registro en la red personal (38);
d) recibir (64) la solicitud de registro (62) desde la estación móvil (26) en la unidad de registro (18) en la unidad de control de sesión de llamada (16) de la red móvil (10) que solicita un registro en la red personal (38);
e) interrogar (66, 72) al servidor de abonado doméstico (20) mediante la unidad de control de sesión de llamada (16) del dominio IMS (14) para información específica de usuario (34) que contiene la identidad de usuario privada (68) encriptada y una dirección (70) y/o un nombre del servidor de gestión de red personal (40),
f) transmitir (72, 74) la identidad de usuario privada (34) encriptada desde el servidor de abonado doméstico (20) al servidor de gestión de red personal (40) mediante la unidad de control de sesión de llamada (18), en donde la identidad de usuario privada (68) encriptada recibida desde el servidor de abonado doméstico (20) y la identidad de usuario pública (36) recibida desde la estación móvil (26) se reenvían (74) desde la unidad de control de sesión de llamada (18) al servidor de gestión de red personal (40) en una solicitud de registro de terceros (73);
g) desencriptar la identidad de usuario privada (68) encriptada recibida en el servidor de gestión de red personal (40);
h) registro de la estación móvil (26) en la red personal (38) mediante el servidor de gestión de red personal (40) usando la identidad de usuario privada (34) desencriptada y la identidad de usuario pública (36).

2. Un método para transmitir información específica de usuario confidencial (34) entre un servidor de abonado doméstico (20) y un servidor de gestión de red personal (40) de acuerdo con la reivindicación 1 **caracterizado por** limitar el periodo de validez de la clave digital (48).

3. Un método para transmitir información específica de usuario confidencial (34) entre un servidor de abonado doméstico (20) y un servidor de gestión de red personal (40) de acuerdo con una de las reivindicaciones 1 a 2 **caracterizado por** comprender el método las etapas de

a) transmitir (76) la identidad de usuario privada (68) encriptada recibida desde el servidor de gestión de red personal (40) al servidor de abonado doméstico (20);
b) transmitir (78) al menos una identidad de usuario pública (36) asignada a la identidad de usuario privada (68) encriptada mediante el servidor de abonado doméstico (20) desde el servidor de abonado doméstico (20) al servidor de gestión de red personal (40); y
c) verificar la identidad de usuario pública (36) recibida desde la unidad de control de sesión de llamada (18) usando la identidad de usuario pública (36) recibida desde el servidor de abonado doméstico (20) mediante el servidor de gestión de red personal (40) durante dicho registro de la estación móvil (26) en la red personal (38).

4. Un método para transmitir información específica de usuario confidencial (34) entre un servidor de abonado doméstico (20) y un servidor de gestión de red personal (40) de acuerdo con una de las reivindicaciones 1 a 3 **caracterizado por** usar una función XOR a nivel de bit para encriptación y desencriptación de la identidad de usuario privada (34).

5. Un sistema para transmitir información específica de usuario confidencial (34) entre un servidor de abonado doméstico (20) y un servidor de gestión de red personal (40) de una red personal (38) en un dominio IMS (14) de una red móvil (10), información (34) que contiene una identidad de usuario privada (34) de una estación móvil (26) usada para un registro de estación móvil que utiliza la red personal (38), que comprende

a) un generador de clave (50) en la red móvil (10) que proporciona una clave digital (48) que es un número aleatorio con la misma longitud de bits que la identidad de usuario privada (34) para el servidor de abonado doméstico (20) y para el servidor de gestión de red personal (40) para encriptar y desencriptar la identidad de usuario privada (34);
b) un módulo de encriptación (44) proporcionado en el servidor de abonado doméstico (20), adaptado para encriptar la identidad de usuario privada (34) en una identidad de usuario privada (68) encriptada, cuyo formato de datos y longitud de datos se corresponden con el formato de datos y la longitud de datos de la identidad de

usuario privada (34) no encriptada;

c) una unidad de registro (18) en una unidad de control de sesión de llamada (16) del dominio IMS (14) para recibir una solicitud de registro (62) que incluye la identidad de usuario privada (34) y una identidad de usuario pública (36) desde la estación móvil (26) que solicita un registro en la red personal (38);

d) un dispositivo (transmisor (46) proporcionado en el servidor de abonado doméstico (20) que transmite la identidad de usuario privada (34) encriptada desde el servidor de abonado doméstico (20) al servidor de gestión de red personal (40), el dispositivo (transmisor (46) adaptado para transmitir la identidad de usuario privada (68) encriptada y una dirección (70) del servidor de gestión de red personal (40) desde el servidor de abonado doméstico (20) a la unidad de control de sesión de llamada (16) para reenviar al servidor de gestión de red personal (40) tras una solicitud desde la unidad de control de sesión de llamada (18);

e) un módulo de desencriptación (54) proporcionado en el servidor de gestión de red personal (40) para desencriptar la identidad de usuario privada (68) encriptada recibida.

f) un dispositivo de registro (42) en el servidor de gestión de red personal (40) que usa la identidad de usuario privada (34) desencriptada y la identidad de usuario pública (36) para registro de la estación móvil (26) en la red personal (38).

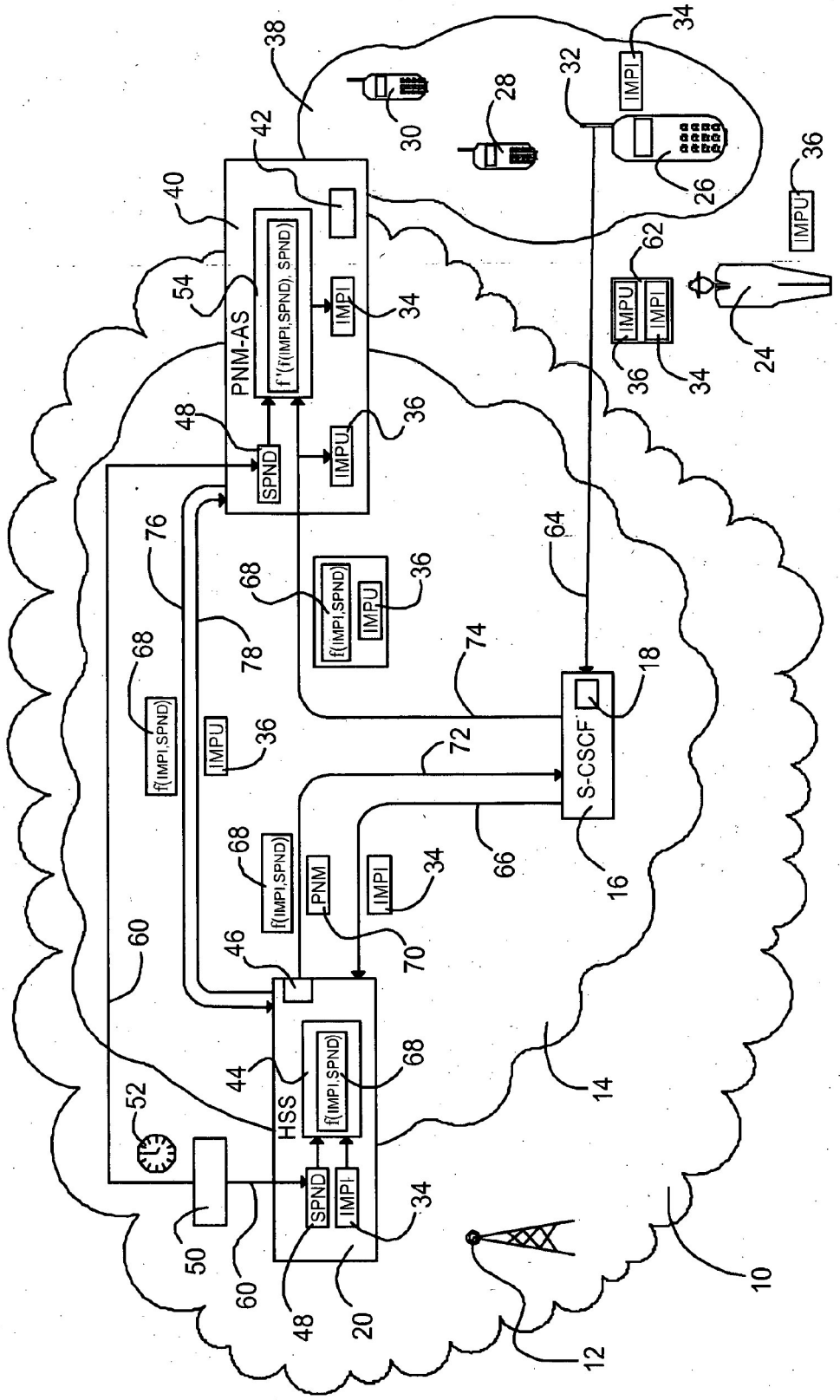
PNM-AS
f''(f(IMPI,SPND), SPND)
SPND
IMPI
IMPU
f(IMPI,SPND)
HSS
PNM
S-CSCF

Fig. 1