(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 559 877**

(51) Int. CI.:

H04L 29/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.02.2011 E 11702044 (6)**

(97) Fecha y número de publicación de la concesión europea: **19.08.2015 EP 2532147**

(54) Título: **Procedimiento de generación de una dirección SIP pública permanente asociada con una identidad privada en una red IMS**

(30) Prioridad:

04.02.2010 EP 10305113

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.02.2016

(73) Titular/es:

GEMALTO SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

FINE, JEAN-YVES

(74) Agente/Representante:

ISERN CUYAS, María Luisa

DESCRIPCIÓN

Procedimiento de generación de una dirección SIP pública permanente asociada con una identidad privada en una red IMS.

El campo de la invención es el de las telecomunicaciones en las redes de transmisión de datos. Más específicamente, la presente invención se refiere a la generación de una dirección SIP pública permanente asociada con una identidad privada de una red IMS (Subsistema Multimedia IP).

Una red IMS es una red IP conectado a una red de acceso. La red IMS proporciona una combinación dinámica de transmisión de voz, vídeo, mensajes, datos, etc. durante la misma sesión. La IMS utiliza el protocolo SIP (Protocolo de Inicio de Sesión) para establecer y controla las comunicaciones o sesiones entre los terminales de usuarios (llamados terminales) o entre los puntos terminales y los servidores de aplicaciones. El SIP permite a un llamante establecer una sesión para el intercambio de paquetes con la persona llamada (usando Agentes Usuarios de SIP, UAS, instalados en los puntos terminales), incluso si el llamante no conoce la dirección IP actual de la persona llamada antes de iniciar la llamada.

Las especificaciones 3GPP IMS actuales requieren el uso de un procedimiento para la autenticación de usuarios en la red IMS. Este procedimiento se describe en 3GPP TS 24.229 y 33.203. Usando este enfoque, la identidad del usuario privado (IMPI) y una o más identidades públicas de los usuarios (IMPU) se asignan al usuario por parte del operador. Para participar en sesiones multimedia, el usuario debe registrar al menos una IMPU en la red. Las identidades se utilizan entonces por la red para identificar al usuario durante el registro y el procedimiento de autenticación (la IMPI se utiliza para localizar la información de abonado, tales como la información de autenticación de usuario, mientras que el modelo de imputación requiere la identidad del usuario con el que el usuario desea interactuar, y a los que los servicios específicos deben ser adjuntados). La IMPI y las IMPU se almacenan en una aplicación llamada Módulo de Identidad de Abonado IMS (ISIM) almacenada en una tarjeta de circuito integrado (UICC) en el terminal de usuario.

Cada IMPU se asocia con un denominado perfil de servicio. El perfil de servicio es un conjunto de servicios y datos relacionados, que incluye, entre otros, los criterios de filtro iniciales que proporcionan una lógica de servicio simple para el usuario (por ejemplo, se define un conjunto de servicios IMS que la identidad pública IMPU podrá utilizar).

La red de acceso a la red IMS es por ejemplo, una red UMTS, LTE, WLAN y/o Internet.

La Figura 1 muestra una red de este tipo IMS conectada a diferentes redes de acceso.

Una red IMS 10, tal como se define por 3GPP TS 23.228, está conectada a los servidores de aplicaciones 11, 12 por las conexiones SIP 13, 14. Los servidores 11 y 12 de alojan las aplicaciones IMS que representan los servicios como la mensajería instantánea, gestión de presencia (usuario presente, ausentes, reunido, ...), del filtro de llamada y las sesiones en tiempo real, tales como voz en la IP (VoIP), videoconferencia, vídeo bajo demanda, compartir videos, juegos en red o televisión a través de IP.

Los usuarios de terminales 15 a 20 acceden a los servicios de la red IMS a través de redes de acceso como una red UMTS 21, una red LTE (Evolución de Largo Plazo) 22, una red 3GPP2 23, una red WLAN 24 o una red de Internet 25. El terminal 17 comunica a través de una conexión inalámbrica 26 con la red LTE 22 y una conexión EV-DO 27 con la red 3GPP2 23.

La red IMS incluye un proxy 28 unido por conexiones SIP 29 a 31 a las pasarelas de interconexión, como una pasarela GGSN (Nodo de Soporte de Pasarela GPRS) 32 particularmente responsable de proporcionar una dirección IP al terminal 15 constituido por un terminal GPRS durante toda la duración de su conexión a la red IMS, una pasarela PDN GW (Pasarela de Red de Paquete de Datos) 33 asegurando el mismo servicio para los terminales LTE 16 y 17, y una pasarela PDSN (Nodo de Servicio de Paquetes de Datos) 34 asegurando una conexión a través de la red 3GPP2 23 del terminal 18 de tipo CDMA 2000.

Se obtiene el acceso a los servicios de la red IMS 10 por los usuarios de los terminales 15-20 después de que estos usuarios estén conectados a sus redes de acceso y hayan solicitado una conexión IP a la red IMS 10. Los terminales pueden igualmente comunicarse entre sí a través de la red IMS, por ejemplo por VoIP.

La autenticación de los terminales por la red IMS 10 se logra gracias a una identidad privada IMPI, generalmente comprendida en una aplicación USIM o ISIM incrustada en los terminales 15 a 20. Cada terminal tiene su propia identidad privada: En el curso de la solicitud para acceder a la red IMS 10, un terminal envía su IMPI a la red 10 y, si es autenticado (en un servidor de registro llamado HSS), le son concedidos los derechos de acceso en función de su perfil y su suscripción. La red IMS procede particularmente a la facturación al usuario y al control de la sesión.

Cada terminal 15-20 también contiene al menos una dirección pública (por tanto no secreta) IMPU que permite a su usuario solicitar y recibir comunicaciones con otros usuarios o acceder a un servicio. Las IMPU se presentan bajo la

forma de un SIP URI (Identificador de Recursos Unificado) como el definido en las recomendaciones IETF RFC 3261 e IETF RFC 2396. A título de ejemplo, una dirección IMPU podría presentarse bajo la forma:

sip: martin@gemalto.como
o también bajo la forma de un número de teléfono:
sip: 0123456789@gemalto.ims.com.

Por el contrario, el formato de una dirección privada IMPI es del tipo:

<xyz>@gemalto.com
siendo <xyz> una cadena de caracteres cualquieras, siendo el formato de una IMPI dicho Identificador de Acceso a la Red, como el que se describe en la recomendación IETF RFC 2486.

Las IMPU y IMPI son típicamente almacenadas en la aplicación ISIM de un terminal, como el descrito en "Servidor Doméstico de Abonado 3GdB" 2008, http://3gdb.org/doc/overview.summary.html. El terminal puede incluir un software que puede registrar las IMPU o dejar al usuario el derecho a registrar las IMPU.

Si el terminal no incluye la aplicación ISIM o USIM, la IMPU y la IMPI se almacenan en una memoria del terminal. En una realización convencional, la ISIM se almacena en un elemento seguro, por ejemplo en una tarjeta de chip UICC extraíble del terminal. Una UICC puede llevar una o más aplicaciones ISIM o USIM. El elemento de seguridad también puede ser parte integrante del terminal.

Después o durante la autenticación de un terminal por el reconocimiento de su IMPI y la verificación de los secretos que dispone, el terminal envía una de sus direcciones IMPU a la HSS de la red IMS 10 con el fin de registrarse y beneficiarse de un servicio de IMS.

El problema que se propone resolver la presente invención es el siguiente: La identidad privada de la IMPI, por ejemplo incluida dentro de una tarjeta inteligente insertada en un terminal móvil, se transmite sólo una vez a la HLR en el procedimiento de autenticación y su formato no permite a la red IMS dirigirse directamente a la tarjeta. Por ello es necesario que los dispositivos móviles modifiquen la IMPI de la tarjeta a una dirección parecida a una IMPU a fin de que la red pueda dirigirse a la tarjeta, por ejemplo para poder actualizar los datos a través de OTA. Esto requiere una modificación y una estandarización de los dispositivos móviles.

Otra solución es que la tarjeta (o la entidad que contiene la IMPI) gestione el proceso de registro con la red IMS. Esto es como tener dos entidades que se registran con el HSS, por una parte el terminal móvil que hace las veces de terminal, y por otras la tarjeta. Dos enlaces seguros IPsec que cooperan con un proxy en la red IMS (del HSS) deben entonces ser establecidos, lo que conduce a una sobrecarga en el proxy y una modificación de la red IMS. Los operadores que gestionan las redes IMS deben entonces agregar estos proxys en sus redes, lo que resulta en costes adicionales.

La presente invención tiene por objetivo principal remediar estos inconvenientes.

Más concretamente, uno de los objetivos de la invención es proporcionar un procedimiento que permita generar una dirección SIP pública permanente asociada con una identidad privada IMPI en una red IMS para que la red pueda hablar directamente y sin divulgación de la identidad privada IMPI con la entidad que contiene esta identidad privada (tarjeta, elemento seguro, terminal, ...).

Este objetivo y otros que aparecerán a continuación, se consiguen gracias a un procedimiento de acuerdo con la reivindicación 1.

La invención también concierne un registro por la red IMS de al menos una dirección pública diferente de la dirección pública permanente, procediendo la red IMS a un registro implícito de la dirección SIP pública permanente conforme a la especificación técnica 3GPP TS 23.228 V8.9.0 de junio 2009.

La función unívoca, no reversible y sin colisiones es preferiblemente un SHA-256.

Otras características y ventajas de la invención aparecerán a partir de la lectura de la siguiente descripción de una forma de realización ventajosa de la invención, dada a título ilustrativo y no limitativo, y de las figuras adjuntas en las que:

- la figura 1 ha sido descrita con referencia al estado de la técnica anterior;
- la figura 2 es un esquema que muestra el funcionamiento del procedimiento según la presente invención.

La figura 1 ha sido descrita anteriormente con referencia al estado de la técnica anterior.

La figura 2 es un esquema que muestra el funcionamiento del procedimiento de acuerdo con la presente invención.

En esta figura, una tarjeta inteligente, por ejemplo con formato ID-0, se encuentra incluida en un terminal 41 constituido por un terminal de telefonía móvil. La tarjeta 40 incluye una ISIM que contiene una identidad privada IMPI. De acuerdo con la invención, se propone aplicar a la identidad privada IMPI una función F unívoca, no reversible y sin colisiones a fin de obtener una dirección SIP pública permanente, calificada $IMPU_{UICC}$. La función F debe ser unívoca para que una IMPI dada, no pueda coincidir con una $IMPU_{UICC}$. También debe ser no reversible, es decir, que conociendo la $IMPU_{UICC}$ no resulte posible deducir la IMPI a partir de la cual se obtuvo, con el fin de mantener la IMPI secreto. Por último, la calidad de no colisión asegura que dirigiendo la tarjeta UICC (como se verá posteriormente) con la $IMPU_{UICC}$ obtenida por la función F, se dirigirá correctamente a la UICC elegida y no a otra UICC que tenga una IMPI diferente.

Se generará así, con la ayuda de la función F, y dentro de la UICC 40, una dirección pública $IMPU_{UICC}$ de la UICC a partir de su identidad privada IMPI.

En una realización preferida, la función F es una función hash de tipo SHA, por ejemplo SHA-256. La aplicación de una función SHA-256 a un bloque de 128 bits, se obtiene de salida una condensación ("hash" en Inglés) de 256 bits. Con tal función F, si un operador crea 2^{128} IMPIs diferentes, la probabilidad de colisión es de 1. A título informativo, una dirección IPV6 mide 16 bytes o 128 bits. Utilizando el argumento teórico de la paradoja de los aniversarios para garantizar que no hay colisión, la salida de la función de hash debe ser mayor o igual a 256 bits. La función SHA-56, por lo tanto es ideal para transformar el formato de una IMPU en un formato de IMPU.

Otra alternativa para la función F es la SHA-1, la SHA-3 o también la Ripend-160 utilizada principalmente en Japón.

Como se indicó anteriormente, con el fin de acceder a un servicio IMS, la UICC 41 transmite una dirección pública IMPU a la red IMS 10 durante o después de la autenticación de la tarjeta 40 (por su IMPI), a través del terminal móvil 41. La red 10 incluye particularmente un servidor de registro HSS señalado como 42 que incluye todos las IMPI e IMPU de los usuarios.

El procedimiento de la invención también se aplica al servidor de registro 42, que, a partir de las diferentes IMPI que contiene, calcula las direcciones SIP $IMPU_{UICC}$ resultantes con la ayuda de la misma función F utilizada en la UICC 40. El servidor de registro 42, por tanto, incluye no sólo las IMPI e IMPU del abonado a la red IMS 10, sino también las $IMPU_{UICC}$ obtenidas por la función F. Al recibir una IMPU, el servidor de registro 42 realiza una operación conocida bajo el nombre de registro implícito: el registro implícito consiste en asociar a una dirección pública IMPU al menos otra dirección pública del mismo abonado. Por ejemplo, si un abonado envía una dirección pública $IMPU_1$ al HSS 42, este HSS 42 registrará no sólo la dirección $IMPU_1$ sino también otras direcciones públicas de ese abonado, señaladas como $IMPU_1$, con el i entero perteneciendo a [2, n], donde n puede ser infinito en teoría. Si, por ejemplo, n = 2, el registro de una dirección pública $IMPU_1$ por el HSS 42 provocará el registro implícito (automático) de las direcciones $IMPU_2$ e $IMPU_3$ de ese abonado.

Más específicamente, las IMPU de un usuario que se pueden agrupar en Conjuntos de Registro Implícito (IRS). Cuando el usuario registra una de sus IMPU en un IRS, todos las otras (no prescritas) IMPU dentro de este RSI son también registradas en la red. Durante el proceso de registro, el terminal del usuario es informado sobre el conjunto completo de las IMPU que han sido registradas de manera implícita en la red como consecuencia del procedimiento de registro. El terminal puede entonces utilizar una de esas IMPU para establecer comunicaciones salientes y puede esperar recibir comunicaciones entrantes a partir de una de sus IMPU. Se hace referencia a la especificación técnica 3GPP TS 23.228 V8.9.0 de junio de 2009 para obtener más información al respecto.

A este respecto, la invención propone asociar con una o varias direcciones públicas IMPU del abonado que comprende una UICC según la invención (comprendiendo la función F) la $IMPU_{UICC}$ de dicho abonado. Así, para un abonado, el simple hecho de solicitar el registro de una de sus direcciones públicas, provocará también el registro de una dirección que corresponde a la de su UICC, a saber $IMPU_{UICC}$. La red IMS es por tanto capaz de dirigir directamente la UICC del abonado, por ejemplo a través de OTA para realizar actualizaciones.

El emparejamiento entre una IMPI y una dirección SIP $IMPU_{UICC}$ se pueden realizar en el HSS 42 fuera de línea o durante una conexión: en modo fuera de conexión, el HSS calcula las direcciones SIP $IMPU_{UICC}$ a partir de las identidades privadas IMPI de los abonados y las asocia en una tabla. Al recibir una IMPI (en una petición de autenticación), el HSS reconoce el IMPI del abonado y sabe de antemano la $IMPU_{UICC}$ que afectará, por el procedimiento de registro implícito descrito anteriormente, a este abonado en una solicitud de registro de una IMPU de ese abonado. En modo conexión, el HSS recibe la IMPI del abonado y calcula entonces (con la ayuda de la función F) la dirección SIP $IMPU_{UICC}$. Esta dirección SIP $IMPU_{UICC}$ puede ser almacenada en correspondencia con la IMPI asociada (de forma permanente, para evitar tener que volver a calcular la $IMPU_{UICC}$ con cada recepción de una IMPI). Esta será registrada por registro implícito con la primera solicitud de registro de una IMPU de ese abonado.

En ausencia de una ISIM en el terminal, la red GPRS utiliza la IMSI y la MSISDN incluidas en la USIM para generar identificadores IMS (IMPI e IMPU) temporales. La invención se aplica también en la medida que esta IMPI temporal

puede ser utilizada para generar $IMPU_{UICC}$.

La invención se aplica tanto si el terminal incluye una UICC como si no: la aplicación ISIM se puede almacenar en un ordenador portátil (20, figura 1) con acceso a internet conectado a la red IMS. La UICC puede igualmente ser reemplazada por un elemento seguro, como por ejemplo un dongle USB.

REIVINDICACIONES

1. Procedimiento de generación de una dirección SIP pública permanente asociada con una identidad privada en una red IMS (10), dicho procedimiento consistente en aplicar a dicha identidad privada una función (F), a fin de obtener dicha dirección SIP pública permanente, **caracterizado porque** dicha función (F) es una función unívoca, no reversible y sin colisiones y **porque** está implementada en un elemento (HSS) de una red IMS (10).

2. Procedimiento de acuerdo con la reivindicación 1, **caracterizado porque** dicha red IMS realiza un registro de al menos una dirección pública diferente de dicha dirección SIP pública permanente, procediendo dicha red a realizar un registro implícito de dicha dirección SIP pública permanente conforme a la especificación técnica 3GPP TS 23.228 V8.9.0 de junio 2009.

3. Procedimiento de acuerdo con una de las reivindicaciones 1 y 2, **caracterizado porque** dicha función unívoca, no reversible y sin colisiones es una SHA-256.

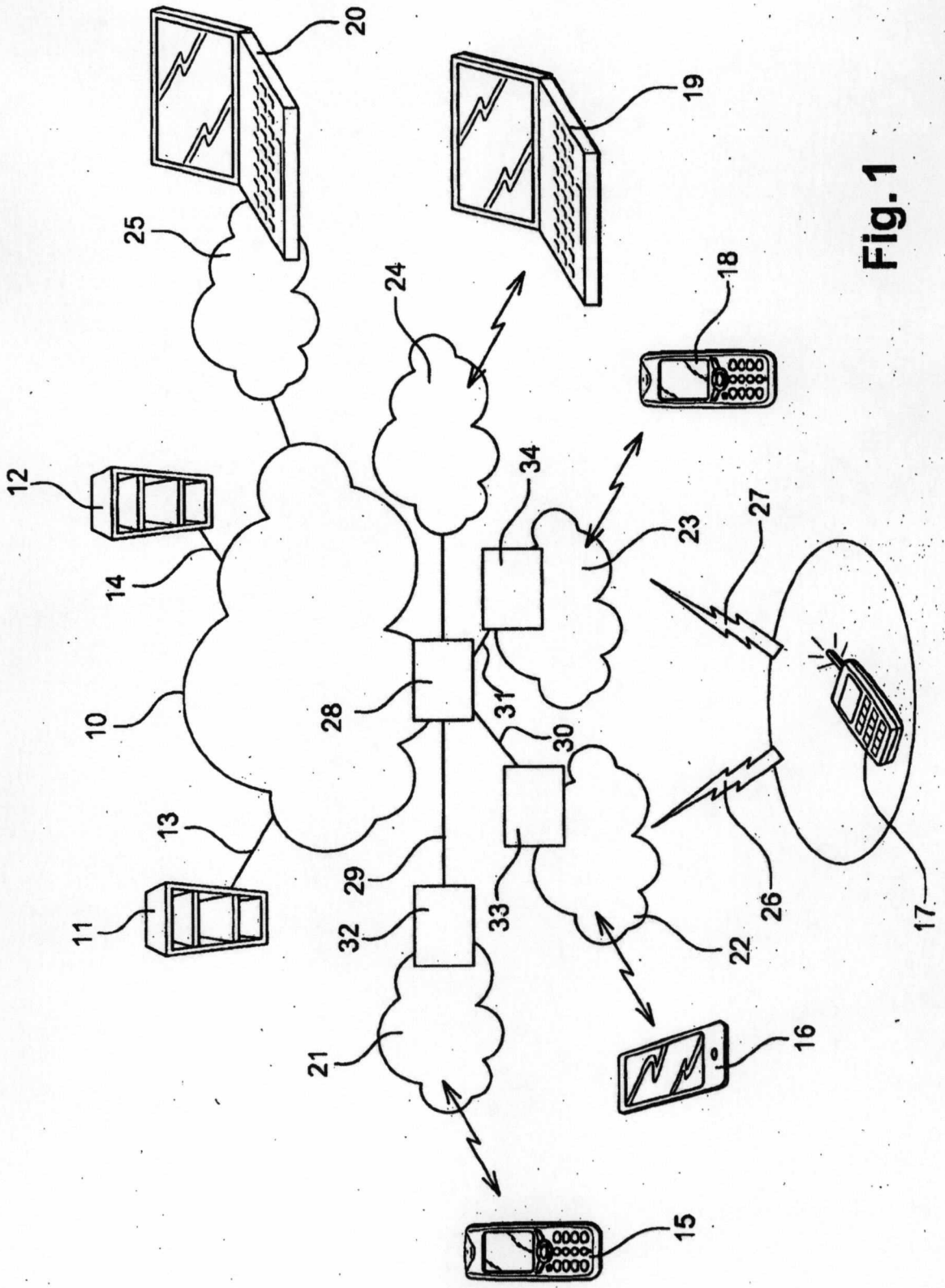
20
19
25
24
18
12
34
23
27
14
10
28
31
30
13
29
33
26
11
32
22
17
21
16
15

Fig. 1

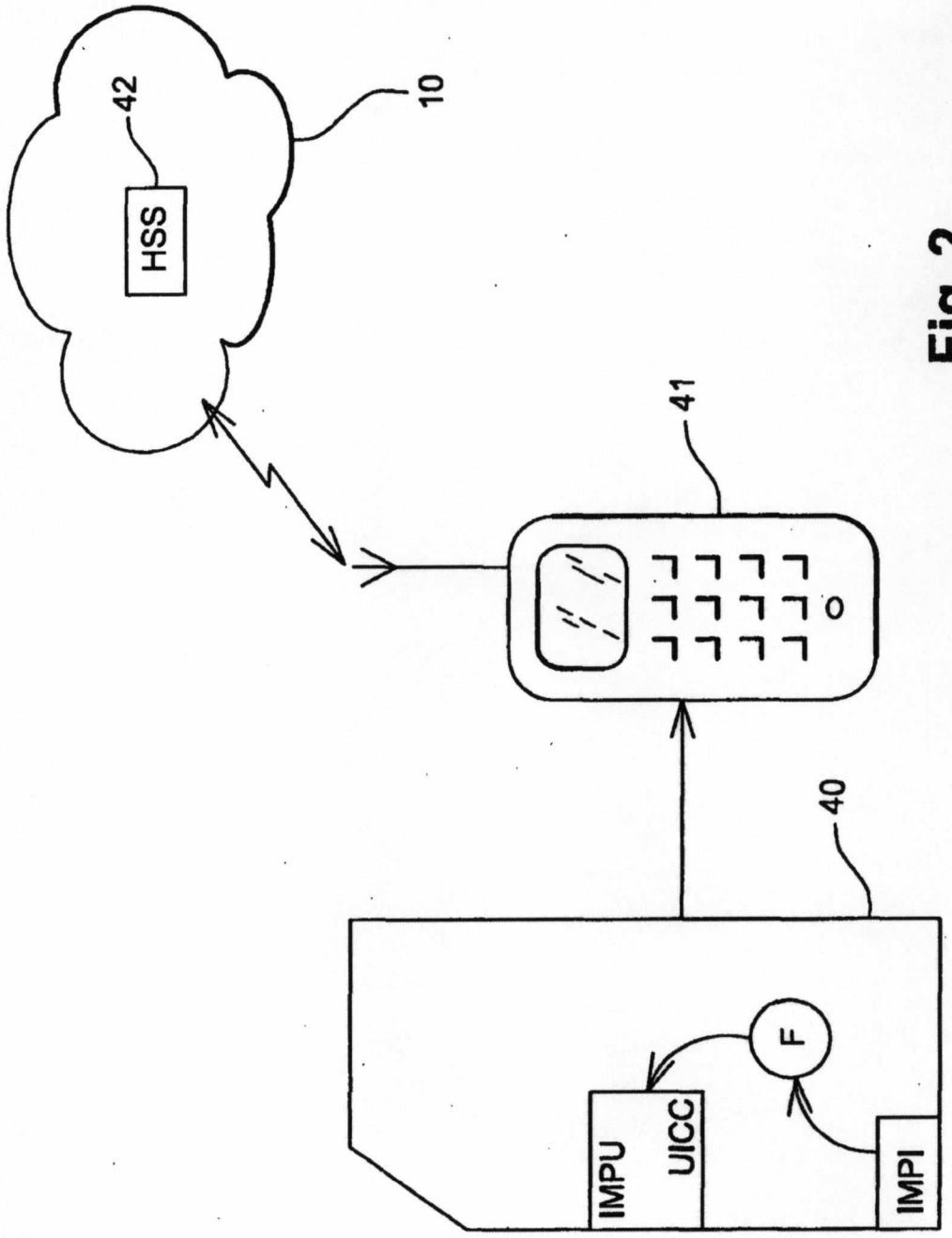

Fig. 2