(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 275 746**

(51) Int. Cl.:
***H04L 29/06*** (2006.01)
***H04Q 3/00*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **01980291 .7**
(86) Fecha de presentación : **28.08.2001**
(87) Número de publicación de la solicitud: **1314296**
(87) Fecha de publicación de la solicitud: **28.05.2003**

(54) Título: **Procedimiento para asegurar un Internet Supplementary Service (servicio suplementario de Internet).**

(30) Prioridad: **31.08.2000 EP 00118893**

(45) Fecha de publicación de la mención BOPI:
**16.06.2007**

(45) Fecha de la publicación del folleto de la patente:
**16.06.2007**

(73) Titular/es: **SIEMENS AKTIENGESELLSCHAFT**
**Wittelsbacherplatz 2**
**80333 München, DE**

(72) Inventor/es: **Mitreuter, Ulrich y**
**Zygan-Maus, Renate**

(74) Agente: **Zuazo Araluze, Alexander**

## DESCRIPCIÓN

Procedimiento para asegurar un Internet Supplementary Service (servicio suplementario de Internet).

1. ¿Qué problema técnico ha de resolverse mediante su invención?

2. ¿Cómo se solucionó este problema hasta ahora?

3. ¿De qué manera resuelve su invención el problema técnico indicado (indique Vd. ventajas)?

Respecto al punto 1: *¿Qué problema técnico ha de resolverse mediante su invención?*

Para la realización de Internet Supplementary Services (servicios suplementarios de Internet), por ejemplo Call Waiting Internet Busy (llamada en espera Internet ocupado), Subscriber Controlled Input via Internet (entrada controlada de abonado vía Internet), se necesitan mensajes (a continuación denominados mensajes de servicios), que a través de la Internet pública son intercambiados entre usuarios de Internet y puestos de conmutación PSTN/ISDN. Así surgen las siguientes exigencias de seguridad:

a) Los recursos de la red de un operador de telecomunicaciones (red PSTN/ISDN, red interna de servidor), deben protegerse frente a un acceso no autorizado (acceso por parte de usuarios de Internet que no son clientes del operador de telecomunicaciones)

b) el emisor de los mensajes de servicios debe ser autentificado y verificada la imposibilidad de falsear los mensajes de servicios

c) el acceso del usuario al servicio debe ser autorizado.

Respecto al punto 2: *¿Cómo se solucionó este problema hasta ahora?*

Procedimientos estándar para el aseguramiento de mensajes de señalización para Internet Supplementary Services (servicios suplementarios de Internet), no existen hasta hoy. En función del servicio, se utilizan hasta ahora distintas combinaciones de procedimientos de aseguramiento IP. En muchos casos se transmite un secreto común (por ejemplo una palabra de paso, un PIN), codificado con procedimientos estándar (por ejemplo "Transport Layer Security", seguridad de capa de transporte, RFC 2246), al servidor, que como Gateway (puerta de acceso) hacia la PSTN/ISDN apoya el servicio. En este servidor se evalúa la palabra de paso, basándose en interfaces con las correspondientes bases de datos referidas al servicio del operador de red PSTN/ISDN, que pueden ser bien bases de datos centrales de la red (en el Gateway Server, servidor de la puerta de acceso, o bien separadamente) o bien bases de datos que se encuentran distribuidas en la red en los puestos de conmutación de abonado. Con tales procedimientos pueden cumplirse las exigencias b) y c), pero no a la vez la exigencia a).

Un ejemplo de un procedimiento de autorización de un ofertante de servicios en una Gateway (puerta de acceso) se encuentra en WO00/30 369.

Respecto al punto 3: *¿De qué manera resuelve su invención el problema técnico indicado (indique Vd. ventajas)?*

El procedimiento de aseguramiento para mensajes de servicios de usuarios de Internet Supplementary Services (servicios suplementarios de Internet) se fracciona en dos etapas parciales. Al acceder Internet a la red del servidor IP del operador de red, se realiza mediante un servidor especial de seguridad (Firewall-Server, servidor de cortafuegos) una autorización genérica, es decir, independientemente del servicio, para la que se utiliza un distintivo independiente del servicio, por ejemplo el número de cliente. A continuación realiza un servidor de acceso a servicios una autorización referida a servicios, para la que se utiliza un secreto referido a servicios (específico de servicios), por ejemplo una palabra de paso de usuario, un PIN. Ni el número de cliente ni el secreto referido a servicios se transmiten a través de Internet (esto se explicará luego más en detalle). Un distintivo de abonado del ISS Subscriber (abonado), por ejemplo el número de llamada, se transmite en el mensaje de servicio en texto explícito (Plaintext) a través de Internet y sirve al receptor (servidor de seguridad o bien servidor de acceso a servicios) para averiguar el correspondiente secreto común (distintivo independiente del servicio o bien secreto referido al servicio), en base al cual el mismo puede comprobar la correspondiente autorización. El servidor de seguridad y el servidor de acceso a servicios pueden en particular también estar realizados sobre una plataforma de hardware.

A continuación se describirá más en detalle la invención (ver al respecto también la figura).

Un distintivo independiente del servicio, por ejemplo el número de cliente del abonado, sirve como secreto común (shared secret) para formar una suma de comprobación criptográfica, por ejemplo según el procedimiento estándar (RFC2104) del "Hashed Message Authentication Code, código de autentificación de mensaje resumido, (abreviadamente HMAC)", que se añade al mensaje de servicios como la llamada "firma digital". Un servidor de seguridad genérico (Firewall-Server, servidor de cortafuegos) evalúa la suma de comprobación HMAC del mensaje de servicios

recibido, basándose en interfaces con las bases de datos del operador de red PSTN/ISDN para números de cliente y números de llamada. Si la comprobación HMAC tiene éxito (con ello se asegura la autentificación del cliente y la integridad de datos) recibe el abonado el acceso a la red del servidor del operador.

Su mensaje es enrutado hacia el servidor de acceso a servicios, que permite el acceso a un Internet Supplementary Service (servicio suplementario de Internet), y aquí tiene lugar la autorización específica del servicio (el servidor de acceso a servicios puede ser en particular un Gateway Server, servidor de puerta de acceso (ver figura), que permite el acceso a un Internet Supplementary Service ofrecido por otra red). Para ello evalúa el servidor de acceso a servicios un segundo "Hashed Message Authentication Code", código de autentificación de mensaje resumido, que ha sido formado por la aplicación ID del usuario con la ayuda de un secreto referido al servicio. El servidor de acceso a servicios evalúa el HMAC basándose en interfaces con las bases de datos referidas al servicio del operador de red PSTN/ISDN que contienen los secretos referidos al servicio de los abonados al servicio. Estas pueden ser bien bases de datos centrales de la red (en el Gateway Server o separadamente) o también bases de datos que se encuentran distribuidas en la red en las interfaces de conmutación de abonados.

*Breve explicación del funcionamiento del HMAC*

El emisor añade al mensaje de servicios antes de su envío el secreto común (aquí por ejemplo número de cliente o palabra de paso de usuario) y forma mediante ambos una suma de comprobación. A continuación se retira el número de cliente o la palabra de paso, se añade la suma de comprobación al mensaje de servicios y se envía el mensaje. El receptor retira la suma de comprobación, añade el número de cliente o la palabra de paso (tomada de su banco de datos) al mensaje de servicios y calcula igualmente la suma de comprobación. Una comparación con éxito de la suma de comprobación recibida con la calculada demuestra primero, que el emisor conoce el número de cliente o la palabra de paso y segundo, que el mensaje no ha sido modificado, en la transmisión (esto habría modificado la suma de comprobación). Por lo tanto, el número de cliente o la palabra de paso no se transmiten ni en texto explícito ni codificados. En lugar de ello, demuestra el emisor que conoce la palabra de paso correcta.

**Ventajas de la invención**

- Mediante el procedimiento de dos etapas descrito es posible cumplir con las exigencias a), b) y c) y a la vez utilizar bases de datos de palabras de paso existentes en los puestos de conmutación y bases de datos del servicio de la red existentes. De esta manera se ahorra la instalación y administración de bancos de datos externos adicionales y la eventual duplicación de datos relevantes para la seguridad (por ejemplo en los puestos de conmutación y en un servidor externo).

- El ISS Subscriber (abonado ISS) no tiene que anotarse ninguna palabra de paso adicional para Internet Supplementary Services, debido a la posibilidad de reutilización de palabras de paso o PINs ya existentes.

- Los bancos de datos internos de los puestos de conmutación no son accesibles desde fuera y con ello son genéricamente más seguros que bancos de datos en servidores.

- Mediante la autentificación en dos etapas se colocan obstáculos adicionales en el camino de los atacantes.

- Los costes de una autorización en dos etapas como la indicada son, debido a la reutilización de bancos de datos ya existentes, claramente inferiores a los de procedimientos de aseguramiento de similar grado de seguridad, que realizan la completa autentificación del abonado ya en el servidor de seguridad a la entrada a la red del servidor IP.

Resumiendo, puede decirse que la invención describe un procedimiento de aseguramiento sencillo de dos etapas, que combina datos existentes (número de cliente, número de llamada) y procedimientos de aseguramiento para redes de telecomunicaciones (PIN referido al número de llamada) con procedimientos de aseguramiento de Internet existentes (HMAC).

## REIVINDICACIONES

1. Procedimiento para el aseguramiento de un Internet Supplementary Service (servicio suplementario de Internet), según el cual

- para el acceso de un mensaje de Internet Supplementary Service (servicio suplementario de Internet) de Internet a una red de servidor IP de un operador de red en un servidor de seguridad, se realiza una autorización independiente del servicio, para la que se utiliza un distintivo independiente del servicio,

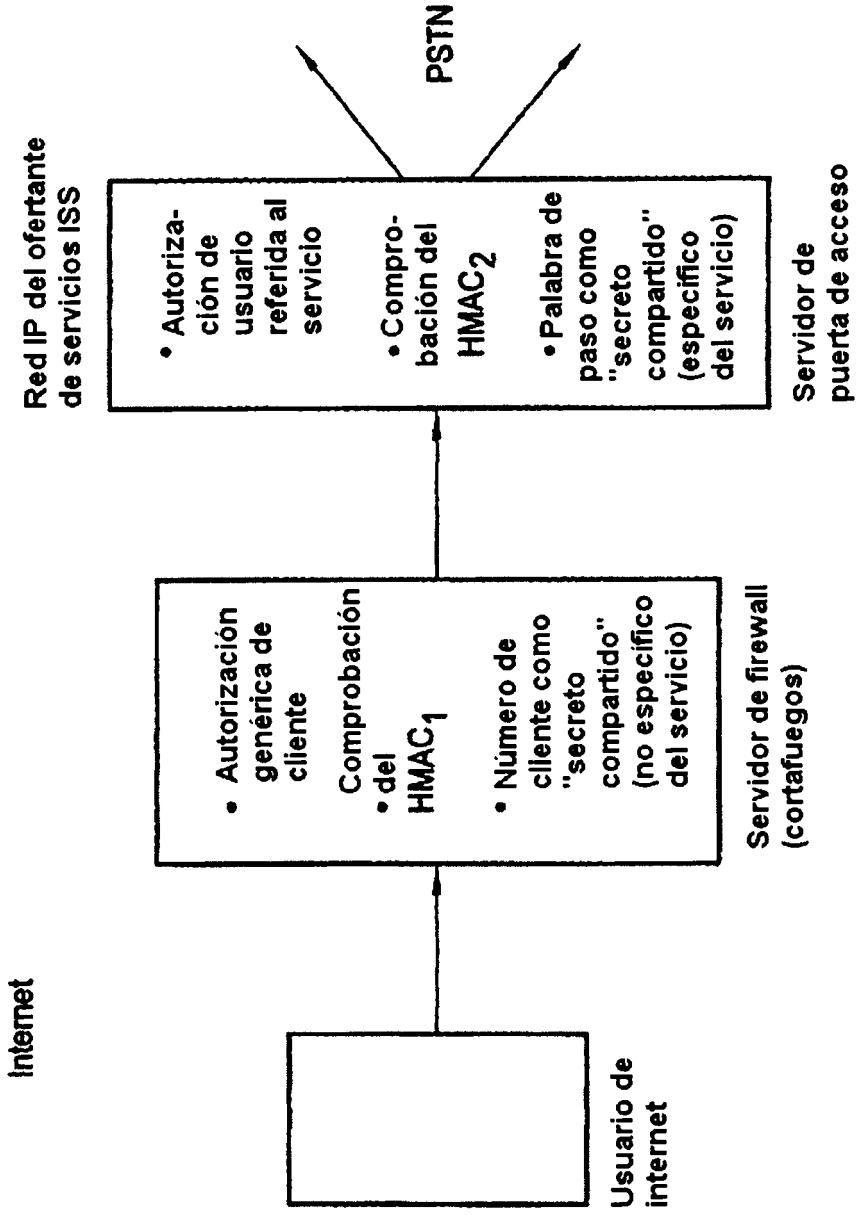
- tras una autorización positiva independiente del servicio en un servidor de acceso a servicios, que permite el acceso a un Internet Supplementary Service, se realiza una autorización referida al servicio, para la que se utiliza un secreto referido al servicio.

2. Procedimiento según la reivindicación 1,

**caracterizado** porque la identificación necesaria en el marco de la autorización independiente del servicio o bien referida al servicio del abonado, se realiza en base a un distintivo de abonado incluido en el mensaje Internet Supplementary Service.

3. Procedimiento según la reivindicación 1 ó 2,

**caracterizado** porque el mensaje Internet Supplementary Service para el acceso de Internet a una red de servidor IP de un operador de red está dotado de una firma digital.


Internet
Usuario de internet
Servidor de firewall (cortafuegos)
• Autorización genérica de cliente
Comprobación del HMAC1
• Número de cliente como "secreto compartido" (no específico del servicio)
Red IP del ofertante de servicios ISS
PSTN
Servidor de puerta de acceso
• Autorización de usuario referida al servicio
• Comprobación del HMAC2
• Palabra de paso como "secreto compartido" (específico del servicio)