(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 424 667**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.11.2010 E 10014689 (3)**

(97) Fecha y número de publicación de la concesión europea: **05.06.2013 EP 2456157**

(54) Título: **Procedimiento y sistema de telecomunicaciones para la protección de la esfera privada durante el anuncio de un usuario en un servicio seguro de la Web por medio de un aparato de telefonía móvil**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.10.2013

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

MILDNER, FRANK;
MESSMER, MARTIN y
FRIESE, INGO

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Procedimiento y sistema de telecomunicaciones para la protección de la esfera privada durante el anuncio de un usuario en un servicio seguro de la Web por medio de un aparato de telefonía móvil

La invención se refiere a un procedimiento para la protección de la esfera privada durante el anuncio de un usuario en la red de telefonía móvil de servicios de la Web así como a un sistema para la realización de tal procedimiento.

Un procedimiento habitual para obtener un acceso a una servicio seguro de la Web por medio de un aparato de telefonía móvil consiste en que el usuario da a conocer su identidad para el inicio de la autentificación a través del navegador de su PC frente a un servicio de la Web. En respuesta, el usuario recibe una llamada palabra de paso una vez, llamada también One Time Passwort (OTP), a través de un mensaje de SMS en su aparato de telefonía móvil. Esta palabra de paso OTP es introducida por el usuario en su navegador, para obtener un acceso al servicio de la Web. Sin embargo, este procedimiento de autentificación conocido no protege la esfera privada del usuario. Además, puede conducir a errores de entrada, puesto que el usuario debe introducir en su PC datos específicos del usuario para la realización de la autentificación.

La invención tiene el cometido de proporcionar un procedimiento así como un sistema de telecomunicaciones para la protección de la esfera privada durante el anuncio de un usuario en un servicio seguro de la Web por medio de un aparato de telefonía móvil, que protege la esfera privada del usuario, excluye en gran medida errores de manejo y es fácil de manipular.

La idea central de la invención se puede ver en que no debe identificarse el usuario en el servicio deseado de la Web, llamado también servicio de la Web, sino que deben identificarse el servicio de la Web deseado y el servicio de autentificación implicado en la autentificación frente al usuario. Otro aspecto de la invención se puede ver en que el usuario no debe introducir datos basados en el usuario en su terminal de telecomunicaciones o aparato de telefonía móvil para la autentificación. De esta manea se pueden excluir errores de manejo. Todo esto se consigue porque la autentificación necesaria para el anuncio del usuario en el servicio seguro de la Web se realiza entre el aparato de telefonía móvil del usuario y un servicio de autentificación. A tal fin, el proceso de autentificación debe iniciarse después de la realización de la identificación del servicio de la Web sólo todavía por el usuario a través de una instrucción de inicio correspondiente.

De acuerdo con otro aspecto, para la realización del proceso de autentificación se tienen en cuenta las Especificaciones técnicas conocidas 3GPP TS 24.109, 3GPP TS 29.109 y 3GPP TS 33.223.

El documento US 2007/220275 publica un procedimiento para el anuncio de un usuario en la red de telefonía móvil de servicios de la Web.

El problema técnico mencionado anteriormente se soluciona, por una parte, por medio de las etapas del procedimiento de la reivindicación 1.

De acuerdo con ello, se define un procedimiento para la protección de la esfera privada durante el anuncio de un usuario en un servicio seguro de la Web por medio de un aparato de telefonía móvil anunciado en un operador de la red de telefonía móvil, en el que está instalada una aplicación de autentificación.

En primer lugar, un usuario solicita un servicio seguro de la Web en el navegador de un terminal de comunicaciones asociado al mismo. En el terminal de comunicaciones se puede tratar de un ordenador personal habitual, un PDA o también un ordenador portátil, que poseen acceso, respectivamente, a Internet. En este lugar hay que indicar que por un servicio seguro de la Web se entiende un servicio de la Web con deber de solicitud o con deber de autentificación.

Un servicio seguro de la Web puede ser solicitado por un usuario de manera convencional, introduciendo, por ejemplo, en el navegador de su terminal de comunicaciones la designación de la fuente correspondiente, en inglés Uniform Ressource Locator (URL) del servicio deseado de la Web. De esta manera, se establece una conexión de comunicación entre el navegador del terminal de comunicaciones y un servicio de autentificación.

Una conexión de comunicaciones de este tipo se puede establecer automáticamente. Pero también es concebible que el servicio solicitado de la Web indique, por ejemplo, un campo “User Login” en el navegador del terminal de comunicaciones, que ofrece la opción de “autentificación a través del aparato de radio móvil”. Si el usuario selecciona esta opción, se desvía un deseo de autentificación correspondiente o una solicitud de anuncio correspondiente al servicio de autentificación.

El servicio de autentificación puede estar instalado en un sistema de autentificación o en un ordenador de autentificación del operador de la red de telefonía móvil, en el que está anunciado el aparato de telefonía móvil, o de otro operador de la red de telefonía móvil. A continuación se transmiten la dirección del servicio de autentificación y una identificación de la sesión, llamada también Session ID, que identifica de una manera unívoca la conexión de

comunicación del usuario con el servicio seguro de la Web, desde el servicio de autentificación hacia el navegador del terminal de comunicaciones. De esta manera, se identifican el servicio de autentificación y el servicio solicitado de la Web frente al usuario y no a la inversa.

En este lugar hay que indicar que existen posibilidades opcionales para comunicar la identificación de la sesión del servicio solicitado de la Web al servicio de autentificación.

De manera ventajosa, la dirección del servicio de autentificación y la identificación de la sesión del servicio seguro de la Web se transmiten en forma de una información codificada, en particular de un código de barras, hacia el navegador del terminal de comunicaciones.

La dirección recibida en el navegador de la instalación de autentificación y la identificación de la sesión recibida del servicio seguro de la Web se transmiten ahora hacia el aparato de telefonía móvil.

En el caso de la transmisión del código de barras, el código de barras se puede transferir por medio de un lector de códigos o de una cámara del aparato de telefonía móvil desde el navegador hacia el aparato de telefonía móvil. No obstante, también es concebible que, por ejemplo, las informaciones codificadas sean transmitidas automáticamente después de la recepción o a través del control del usuario desde el navegador, por ejemplo, a través de una interfaz de Bluetooth hacia el aparato de telefonía móvil.

La aplicación de autentificación del aparato de telefonía móvil evalúa la dirección del servicio de autentificación y transmite una solicitud de autentificación, que contiene en primer lugar una consulta de autentificación y un número de identificación del usuario anunciado a través del aparato de telefonía móvil, hacia el servicio de autentificación.

Con preferencia, también se puede evaluar todavía la identificación de la sesión del servicio de la Web solicitado. La solicitud de autentificación se puede transmitir después de la autorización a través del usuario, por ejemplo a través de simple confirmación o también a través de la entrada de un PIN en el aparato de telefonía móvil. A través de la consulta de autentificación se solicita al servicio de autentificación que inicie el procedimiento de autentificación. La solicitud de autentificación se transmite a través de la red de telefonía móvil del operador de la red de telefonía móvil, en el que está anunciado el aparato de telefonía móvil.

Como reacción a la consulta de autentificación, el servicio de autentificación provoca la realización de una autentificación segura entre el aparato de telefonía móvil y el servicio de autentificación. Cuando la autentificación de ha realizado con éxito, el servicio de autentificación genera una palabra de paso y transmite esta palabra de paso, con preferencia sobre la base reconsultas asíncronas periódicas del navegador, al navegador del terminal de comunicaciones. Es importante indicar que la palabra de paso no contiene datos específicos del usuario.

En la palabra de paso se puede tratar de una palabra de paso una vez, una llamada One-Time-Token.

Para anunciarse en el servicio seguro de la Web, se transmite ahora la palabra de paso desde el navegador hacia el servicio seguro de la Web.

En virtud de una relación de confianza entre el servicio de la Web y el servicio de autentificación, el servicio de la Web puede validar ahora la palabra de paso en el servicio de autentificación.

De manera alternativa, la palabra de paso puede ser transmitida desde el servicio de autentificación también hacia el servicio seguro de la Web, verificando el servicio de la Web entonces la coincidencia de la palabra de paso recibida por el servicio de autentificación y la palabra de paso recibida por el navegador del terminal de comunicaciones.

En el caso de una autentificación segura del aparato de telefonía móvil en el servicio de autentificación, se puede tratar de una manera más conveniente de un procedimiento de Pregunta-Respuesta (Challenge-Response).

De manera más ventajosa, el servicio de autentificación solicita informaciones necesarias para la realización del procedimiento de Pregunta-Respuesta desde el operador de la red de telefonía móvil, en el que está anunciado el aparato de telefonía móvil del usuario.

De acuerdo con una forma de realización ejemplar, la autentificación se realiza entre el servicio de autentificación, el operador de telefonía móvil y el aparato de telefonía móvil de acuerdo con la Especificación 3GPP TS 33.223.

De acuerdo con un desarrollo conveniente, la solicitud de autentificación generada por la aplicación de autentificación del aparato de telefonía móvil contiene, además, la dirección del servicio de autentificación y la identificación de la sesión del servicio seleccionado de la Web.

El problema técnico mencionado anteriormente se soluciona de la misma manera a través de las características de la reivindicación 9.

De acuerdo con ello, se acondiciona un sistema de telecomunicaciones para la protección de la esfera privada

durante el anuncio de un usuario en un servicio seguro de la Web por medio de un aparato de telefonía móvil.

El sistema de telecomunicaciones presenta una plataforma, que proporciona al menos un servicio seguro de la Web. Además, está previsto un terminal de comunicaciones asociado al usuario, en el que está inicializado un navegador. Por medio del navegador, el usuario puede solicitar un servicio seguro de la Web. El sistema de telecomunicaciones contiene, además, un aparato de telefonía móvil anunciado en un operador de la red de telefonía móvil, en el que está instalada la aplicación de autentificación. Además, está previsto un servicio de autentificación, que se comunica a través de una primera interfaz de comunicaciones con el navegador del terminal de comunicaciones y a través de una segunda interfaz de comunicaciones con la aplicación de autentificación del terminal de telefonía móvil. El servicio de autentificación está instalado de una manera conveniente en un sistema de autentificación separado del operador de telefonía móvil, en el está anunciado el aparato de telefonía móvil, o de otro operador de la red de telefonía móvil. El servicio de autentificación está configurado para transmitir la dirección del servicio de autentificación y la identificación de la sesión de un servicio seguro de la Web seleccionado en el navegador hacia el navegador. El sistema de telecomunicaciones comprende, además, una instalación para la transmisión de la dirección del servicio de autentificación y de la identificación de la sesión del servicio solicitado de la Web hacia la aplicación de autentificación del aparato de telefonía móvil. La aplicación de autentificación del aparato de telefonía móvil genera, como reacción a la dirección recibida del servicio de autentificación, un anuncio de autentificación, que contiene una solicitud de autentificación y un número de identificación del aparato de telefonía móvil. Transmite este anuncio de autentificación a través de una red de telefonía móvil hacia el servicio de autentificación. Para asegurar la protección de la esfera privada durante el anuncio del usuario en el servicio seguro de la Web, el servicio de autentificación y la aplicación de autentificación del aparato de telefonía móvil están configurados para la realización de una autentificación segura. Después de la realización con éxito de la autentificación, el servicio de autentificación genera una palabra de paso y transmite esta palabra de paso a través de la primera interfaz de comunicaciones hacia el navegador del terminal de comunicaciones. El navegador está configurado para transmitir la palabra de paso automáticamente o con la conformidad del usuario hacia al servicio de la Web. Como reacción a la palabra de paso recibida, el servicio de la Web libera el acceso para el usuario. El usuario se puede anunciar de esta manera, por ejemplo, anónimo en el servicio seguro de la Web.

De manera ventajosa, el servicio de autentificación y la aplicación de autentificación del aparato de telefonía móvil están configurados para la realización de un procedimiento de Pregunta-Respuesta.

De acuerdo con un desarrollo ventajoso, el servicio de autentificación se comunica a través de una tercera interfaz de comunicaciones con una instalación de autentificación del operador de telefonía móvil, en el que está anunciado el aparato de telefonía móvil, para recibir la información necesaria para el procedimiento de Pregunta-Respuesta.

De acuerdo con una forma de realización ventajosa, el servicio de autentificación, la aplicación de autentificación del aparato de telefonía móvil y la instalación de autentificación del operador de la red de telefonía móvil están configurados para la realización de una autentificación de acuerdo con la Especificación 3GPP TS 33.223. En este caso, en la instalación de autentificación está instalada una Función de Servidor Autoelevador (BSF).

De manera ventajosa, la validación de la palabra de paso, que recibe el servicio de la Web desde el terminal de comunicaciones, se realiza a través del servicio de la Web por medio de una interfaz de comunicaciones de confianza del servicio de autentificación.

La palabra de paso puede ser una llamada palabra de paso una vez (One-Time-Token).

En el número de identificación del usuario del aparato de telefonía móvil se puede tratar de un número IMSI o número MSISDN. El acrónimo IMSI representa International Mobil Subscriber Identity, mientras que el acrónimo MSISDN representa Mobil Subscriber ISDN. El significado y la función de estos números de identificación se conocen en general.

El servicio de autentificación y la plataforma pueden pertenecer al operador de telefonía móvil, en el que está anunciado el aparato de telefonía móvil, o a otro operador de telefonía móvil.

La invención se explica a continuación con la ayuda de un ejemplo de realización en combinación con los dibujos adjuntos. En este caso:

La figura 1 muestra la estructura de principio de un sistema de telecomunicaciones, en el que está realizada la invención, y

La figura 2 muestra el ciclo de comunicación para la protección de la esfera privada durante el anuncio de un usuario en un servicio seguro de la Web por medio de un aparato de telefonía móvil.

La figura 1 muestra un sistema de telecomunicaciones ejemplar 10, en el que está realizada la invención. El sistema de telecomunicaciones 10 comprende, por ejemplo, un sistema de autentificación 30, en el que está instalado un servicio de autentificación 34. El servicio de autentificación 34 está configurado para realizar una función de

autentificación, para posibilitar a un usuario una protección de la esfera privada durante el anuncio en un servicio de la Web. El sistema de autentificación 30 presenta una primera interfaz de comunicaciones 33, llamada también Proxy, a través de la cual el servicio de autentificación 34 se puede comunicar con un ordenador personal 50 de un usuario. En particular, en el ordenador personal está instalado un navegador 51, que se puede comunicar a través de la interfaz de comunicaciones 33 con el servicio de autentificación 34.

Además, está prevista una plataforma de servidor de la Web 40, en la que se realiza el al menos un servicio seguro de la Web 41. A cada servicio de la Web está asociada una dirección, un llamado Uniform-Ressource-Locator (URL), con cuya ayuda el usuario puede solicitar en el navegador 51 el servicio correspondiente de la Web. El servicio de autentificación 34 del sistema de autentificación 30 se puede comunicar a través de otra interfaz de comunicación 35 con el servicio de la Web 41. La interfaz de comunicación 33 puede estar configurada como interfaz http o interfaz https. La comunicación entre el sistema de autentificación 30, el servicio de la Web 41 y el PC 50 se realiza a través de comunicaciones de Internet correspondientes.

El sistema de telecomunicaciones 10 contiene, además, al menos un aparato de telefonía móvil 60, que pertenece al usuario del ordenador personal 50. El aparato de telefonía móvil 60, que puede ser un teléfono móvil, presenta de manera conocida en sí una tarjeta SIM 62, a la que está ahocicada una identificación unívoca, por ejemplo en forma de un número IMSI o de un número MSISDN. En el aparato de telefonía móvil 60 está instalado un cliente de autentificación 61, llamado también aplicación de autentificación. Para la presente invención no tiene importancia si la aplicación de autentificación 61 está instalada en el aparato de telefonía móvil 60 o en la tarjeta SIM 62. Además, el aparato de telefonía móvil 60 contiene un lector de códigos de barras y/o una cámara 63. El sistema de autentificación 30 dispone de otra interfaz de comunicación 32, a través de la cual el servicio de autentificación 34 se puede comunicar con la aplicación de autentificación 61 del aparato de telefonía móvil 60. La interfaz de comunicación 32 puede estar implementada como combinación de interfaz-Ua y de interfaz-Upa, que se especifica en la Especificación técnica 3 GPP TS33.223. Como se explica todavía en detalle a continuación, la aplicación de autentificación 61 puede generar mensajes de solicitud de impulso, con los que se puede solicitud al servicio de autentificación 34 que inicie un proceso de autentificación.

La comunicación entre el servicio de autentificación 34 y la aplicación de autentificación 61 del aparato de telefonía móvil 60 se realiza a través de una red de telefonía móvil en la que el usuario está anunciado a través del aparato de telefonía móvil 60. Se supone que el usuario está anunciado en el operador de la red de telefonía móvil 20. Para poder realizar una autentificación, el sistema de autentificación 30 puede presentar otra interfaz de comunicación 31, a través de la cual el servicio de autentificación 34 se puede comunicar con una instalación de autentificación 21 del operador de la red de telefonía móvil 20. A tal fin, la interfaz de comunicaciones 31 está implementada con preferencia como interfaz-Zpn, que está normalizada de acuerdo con la Especificación técnica 3GPP TS29.109. En este caso, en la instalación de autentificación 21 está instalada la Función de Servidor de Autoelevador (Bootstrapping Server Function) y el servicio de autentificación 34 puede solicitar, de acuerdo con el procedimiento de empuje 3GPP GBA una información de Pregunta-Respuesta, llamada también información de empuje GBA (GPI), desde la instalación de autentificación 21.

El sistema de telecomunicaciones 10 puede comprender otras redes de telefonía móvil de otros operadores de telefonía móvil. Para una representación más sencilla, solamente se representa otro operador de la red de telefonía móvil 150, que dispone de la misma manera de una instalación de autentificación 151 con una funcionalidad de Función de Servidor de Autoelevador. Los operadores de telefonía móvil 20 y 150 operan de manera conocida en sí un sistema de usuarios Heimat 22 y 152, respectivamente, llamado también Home-Subscriber-System. Cada Home-Subscriber-System administra de manera conocida en sí los datos de los aparatos de telefonía móvil anunciados respectivos. El Home-Subscriber-System 22 administra, entre otros, los datos del usuario del aparato de telefonía móvil 60.

El modo de funcionamiento del sistema de telecomunicaciones ejemplar mostrado en la figura 1 se explica en detalle ahora con la ayuda de un ejemplo de realización en combinación con la figura 2.

En primer lugar, se supone que el sistema de autentificación 30 y la plataforma 40 son operados por el operador de la red de telefonía móvil 150. El usuario o bien el aparato de telefonía móvil 60 son abonados del operador de la red de telefonía móvil 20.

A continuación, el usuario del ordenador personal 50 quisiera recibir un acceso al servicio seguro de la Web 41, pero sin tener que identificarse frente al servicio de la Web 41.

A tal fin, como se muestra en la figura 2, el usuario puede introducir en el navegador 51 una solicitud de servicio de la Web 70, que contiene entre otras cosas el URL del servicio de la Web 41. Como resultado se puede mostrar una página del servicio de la Web con una solicitud de autentificación 75 en el navegador 51, que contiene un campo de anuncio con la opción “autentificación a través del aparato de telefonía móvil”. Si el usuario selecciona esta forma de autentificación en el navegador 51, se conecta el navegador 51 a través de la interfaz de comunicaciones 33 con el servicio de autentificación 34. El navegador 51 transmite ahora un mensaje de solicitud de autentificación hacia el

servicio de autentificación 34. Con otras palabras, el navegador 51 se desvía, como reacción a la forma de autentificación seleccionada, hacia el servicio de autentificación 34. El servicio de autentificación 34 dispone de una función de autentificación correspondiente que, como reacción al mensaje de solicitud de autentificación 80, genera un mensaje de respuesta 85, que contiene la dirección del servicio de autentificación 34 y la identificación de la sesión del servicio de la Web 41. El mensaje 85 es transmitido con preferencia en forma de un código de barras desde el servicio de autentificación 34 hacia el navegador 51.

El servicio de autentificación 34 puede recibir la identificación de la sesión del servicio de la Web 41 solicitado de diferentes maneras. Es concebible que el navegador 51 transmita con el mensaje 80 también el URL del servicio de la Web 41 solicitado hacia el servicio de autentificación 34. El servicio de autentificación 34 solicita entonces él mismo la identificación de la sesión desde el servicio de la Web 41.

Para poder realizar la protección de la esfera privada durante el anuncio, el usuario del operador de la red de telefonía móvil 20 puede asumir el código de barras recibido por medio del lector de códigos de barras 63 o de la cámara 63 en el aparato de telefonía móvil 60. La transmisión del código de barras se representa en la figura 2 en la etapa 90. La aplicación de autentificación 61 del aparato de telefonía móvil 60 está en condiciones de obtener la identificación de la sesión y la dirección del servicio de autentificación 34 desde el código de barras. Como reacción a la dirección del servicio de autentificación 34 obtenida en el código de barras, la aplicación de autentificación 61 genera un mensaje de solicitud de autentificación 95, que contiene, por ejemplo, el número MSISDN de la tarjeta SIM 62 del aparato de telefonía móvil 60, la identificación de la sesión del servicio de la Web 41 y la dirección del servicio de autentificación 34. Este mensaje de solicitud de la autentificación 95 transmite la aplicación de autentificación 61 a través de la red de telefonía móvil del operador de la red de telefonía móvil 20 hacia la interfaz 32 del sistema de autentificación 30.

Como reacción al mensaje de solicitud de autentificación 95 recibido, el servicio de autentificación 34 transmite un mensaje de solicitud 100 a través de la interfaz 31 del ordenador de autentificación 30 hacia la instalación de autentificación 21 del operador de la red de telefonía móvil 20, en el que está anunciado el aparato de telefonía móvil 60. En el ejemplo descrito, el mensaje de solicitud 100 contiene una solicitud GPI a la Función de Servidor de Autoelevador de la instalación de autentificación 21 para transmitir una información GPI hacia el servicio de autentificación 34. En la información GPI se trata de una información de empuje GBA (GPI) de acuerdo con la Especificación técnica 3GPP TS 33.223. La información GPI contiene, expresado de forma sencilla, claves relacionadas con el usuario, la pregunta y la respuesta correspondiente para el procedimiento de Pregunta-Respuesta, que debe realizarse entre el servicio de autentificación 34 y la aplicación de autentificación 61 del aparato de telefonía móvil 60. La instalación de autentificación 21 puede solicitar estas informaciones a través del Home Subscriber System 22 del operador de la red de telefonía móvil 20. A continuación, la instalación de autentificación 21 o bien su función de servidor de autoelevador transmite la información GPI a través de la interfaz de comunicación 31 hacia el servicio de autentificación 34. El servicio de autentificación 34 transmite entonces la pregunta contenida en la información GPI en un mensaje 110 a través de la interfaz de comunicación 32 y la red de telefonía móvil del operador de la red de telefonía móvil 20 hacia la aplicación de autentificación 61 del aparato de telefonía móvil 60. Si la aplicación de autentificación 61 está instalada en el aparato de telefonía móvil 60 y no en la tarjeta SIM 62, la aplicación de autentificación 61 transmite la pregunta a la tarjeta SIM 62. La tarjeta SIM 62 verifica de manera conocida en sí (por ejemplo, a través de la aplicación USIM), si en la respuesta recibida se trata de una consulta correcta. De esta manera, la tarjeta SIM 62 puede verificar la identidad del operador de la red de telefonía móvil 20. La tarjeta SIM 62 genera en el caso de una verificación con éxito con su clave la respuesta que pertenece a la pregunta y la transmite, por ejemplo, en un mensaje codificado 115 por medio del terminal móvil 60 de retorno al servicio de autentificación 34. En el sistema de autentificación 30 está registrada la respuesta GPI del MNO 20, con la que el servicio de autentificación 34 compara la respuesta recibida. Si el servicio de autentificación 34 puede comparar la respuesta con éxito, entonces la autentificación del usuario es valuado como exitosa. Como reacción a la autentificación con éxito y, si está implementada de manera ventajosa, sobre la base de consultas asíncronas periódicas 87 del navegador, el servicio de autentificación 34 transmite una palabra de paso, que puede ser una palabra de paso una vez segura, en un mensaje 125 a través de la interfaz de comunicaciones 33 hacia el navegador 51 del ordenador personal 50 del usuario. El navegador 51 transmite entonces la palabra de paso recibida desde el servicio de autentificación 34 en un mensaje 130 hacia el servicio de la Web 41. El servicio de la Web 41 valida la palabra de paso en un mensaje 120 en el servicio de autentificación 34 como solicitud o autentificación admisible del usuario frente al servicio de la Web 41.

De manera alternativa, el servicio de autentificación 34 puede transmitir la palabra de paso una vez transmitida hacia el navegador 51 en un mensaje 120 a través de la interfaz de comunicaciones 33 o la otra interfaz 35 también hacia el servicio de la Web 41. El servicio de la Web 41 compara entonces la palabra de paso una vez recibida desde el servicio de autentificación 34 con la palabra de paso una vez recibida desde el navegador 51 para determinar la coincidencia. Si las dos palabras de paso coinciden, el cliente se considera autentificado.

De esta manera, el cliente del operador de la red de telefonía móvil 20 se puede anunciar con seguridad y con protección de la esfera privada en el servicio de la Web 41.

Este objetivo se consigue especialmente porque el aparato de telefonía móvil 60 posee un cliente de autentificación 61, que puede transmitir un mensaje de solicitud de autentificación 95 hacia el servicio de autentificación 34. El servicio de autentificación 34 contiene una función de autentificación configurada de forma correspondiente, que puede recibir el mensaje de solicitud de autentificación desde el cliente de autentificación 61 del aparato de telefonía móvil. Además, el servicio de autentificación, como reacción al mensaje de solicitud de autentificación, recibe automáticamente las informaciones de pregunta-respuesta correspondientes desde el operador de la red de telefonía móvil 20, al que pertenece el usuario del aparato de telefonía móvil 60, y lleva a cabo a continuación una autentificación con el aparato de telefonía móvil, sin que el usuario deba identificarse personalmente en el servicio de la Web.

De esta manera, se garantiza una autentificación sencilla y segura para el usuario y la protección de la esfera privada, puesto que no se requiere del usuario ninguna entrada manual de informaciones de identificación y la autentificación frente al servicio de la Web se realiza, por ejemplo, de forma anónima.

REIVINDICACIONES

1.- Procedimiento para la protección de la esfera privada durante el anuncio de un usuario en un servicio seguro de la Web (41) por medio de un aparato de telefonía móvil (60) anunciado en un operador de la red de telefonía móvil (20), en el que está instalada una aplicación de autentificación (61), con las etapas siguientes:

- solicitud de un anuncio seguro de la Web (41) en un navegador (51) de un terminal de comunicaciones (50) del usuario;
- establecimiento de una conexión de comunicaciones entre el navegador (51) del terminal de comunicaciones (50) y un servicio de autentificación (34);
- transmisión de la dirección del servicio de autentificación (34) y de la identificación de la sesión del servicio seguro de la Web (41) desde el servicio de autentificación (34) hacia el navegador (51) del terminal de comunicaciones (50);
- transmisión de la dirección de la instalación de autentificación (34) y de la identificación de la sesión del servicio seguro de la Web (41) al aparato de telefonía móvil (60);
- como reacción a la dirección del servicio de autentificación (34), transmisión de un anuncio de autentificación, que contiene una solicitud de autentificación y un número de identificación del aparato de telefonía móvil (60), desde la aplicación de autentificación (61) del aparato de telefonía móvil (60) hacia el servicio de autentificación (34);
- realización de una autentificación segura entre el servicio de autentificación (34) y el aparato de telefonía móvil (60),
- generación de una palabra de paso a través del servicio de autentificación (34), cuando la autentificación se ha realizado con éxito;
- transmisión de la palabra de paso hacia el navegador (51) del terminal de comunicaciones (50);
- anuncio del usuario en el servicio seguro de la Web (41), siendo transmitida la palabra de paso desde el navegador (51) hacia el servicio seguro de la Web (41).

2.- Procedimiento de acuerdo con la reivindicación 1, caracterizado porque como autentificación segura se realiza un procedimiento de Pregunta-Respuesta.

3.- Procedimiento de acuerdo con la reivindicación 2, caracterizado porque el servicio de autentificación (34) solicita las informaciones de autentificación necesarias para la realización del procedimiento de Pregunta-Respuesta desde el operador de la red de telefonía móvil (20), en el que se ha anunciado el aparato de telefonía móvil (60).

4.- Procedimiento de acuerdo con la reivindicación 2 ó 3, caracterizado porque la autentificación se realiza de acuerdo con la Especificación 3GPP TS 33.223.

5.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, caracterizado porque la palabra de paso es transmitida desde el servicio de autentificación (34) también al servicio seguro de la Web (41) y porque el servicio de la Web (41) verifica la coincidencia de la palabra de paso recibida desde el navegador (51) del terminal de comunicaciones (50).

6.- Procedimiento de acuerdo con una de las reivindicaciones 1 a 5, caracterizado porque el servicio de la Web (41) recibe la palabra de paso desde el navegador (51) del terminal de comunicaciones (50) y la valida en el servicio de autentificación (34).

7.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, caracterizado porque la dirección del servicio de autentificación (34) y de la identificación de la sesión del servicio seguro de la Web (41) se transmite en forma de una información codificada, en particular de un código de barras, hacia el navegador (51) del terminal de comunicaciones y se transmite por medio de un lector de códigos (63) o de una cámara (63) del aparato de telefonía móvil (60) al aparato de telefonía móvil.

8.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, caracterizado porque el anuncio de autentificación generado por la aplicación de autentificación (61) contiene, además, la dirección del servicio de autentificación y la identificación de la sesión del servicio seleccionado de la Web (41).

9.- Sistema de telecomunicaciones (10) para la protección de la esfera privada durante el anuncio de un usuario en un servicio seguro de la Web (41) por medio de un aparato de telefonía móvil (60), con una plataforma (40) que proporciona al menos un servicio seguro de la Web (41), con un terminal de comunicaciones (50) asociado al

usuario, en el que está instalado un navegador (51), con un aparato de telefonía móvil (60) anunciado en un operador de la red de telefonía móvil (20) y asociado al usuario, en el que está instalada una aplicación de autentificación (61), con un servicio de autentificación (34), que se comunica a través de una primera interfaz de comunicaciones (33) con el navegador (51) del terminal de comunicaciones (50) y a través de una segunda interfaz de comunicaciones (33) con la aplicación de autentificación del aparato de telefonía móvil (60), en el que el servicio de autentificación (34) está configurado para la transmisión de la dirección del servicio de autentificación (34) y de la identificación de la sesión de un servicio seguro de la Web (41) seleccionado en el navegador (51) hacia el navegador (51), en el que está prevista una instalación (63) para la transmisión de la dirección del servicio de autentificación (34) y de la identificación de la sesión del servicio seguro de la Web (41) seleccionado en el navegador para la aplicación de autentificación (61) del aparato de telefonía móvil (60), en el que la aplicación de autentificación (61) del aparato de telefonía móvil (60) genera, como reacción a la dirección recibida del servicio de autentificación (34) una solicitud de autentificación, que contiene una solicitud de autentificación y un número de identificación del aparato de telefonía móvil (60) y la transmite a través de una red de telefonía móvil hacia el servicio de autentificación (34), en el que el servicio de autentificación (34) y la aplicación de la autentificación (61) del aparato de telefonía móvil (60) están configurados para la realización de una autentificación segura, en el que el servicio de autentificación (34) genera después de una autentificación realizada con éxito una palabra de paso y la transmite a través de la primera interfaz de comunicación (33) hacia el navegador (51) del terminal de comunicación (50), en el que el navegador (51) está configurado para la transmisión de la palabra de paso hacia el servicio de la Web (41), y en el que el servicio de la Web (41) libera el acceso para el usuario como reacción a la palabra de paso recibida.

10.- Sistema de telecomunicaciones de acuerdo con la reivindicación 9, caracterizado porque el servicio de autentificación (34) y la aplicación de autentificación (61) del aparato de telefonía móvil (60) están configurados para la realización de un procedimiento de Pregunta-Respuesta.

11.- Sistema de telecomunicaciones de acuerdo con la reivindicación 10, caracterizado porque el servicio de autentificación (34) se comunica a través de una tercera interfaz de comunicaciones (31) con una instalación de autentificación (21) del operador de telefonía móvil (20), en el que está anunciado el aparato de telefonía móvil (60), para obtener la información necesaria para el procedimiento de Pregunta-Respuesta.

12.- Sistema de telecomunicaciones de acuerdo con una de las reivindicaciones 9 a 11, caracterizado porque el servicio de autentificación (34) transmite la palabra de paso a través de la segunda interfaz de comunicaciones (33) también hacia el servicio de la Web (41).

13.- Sistema de telecomunicaciones de acuerdo con una de las reivindicaciones 9 a 12, caracterizado porque la palabra de paso es una palabra de paso una vez (One-Time-Token).

14.- Sistema de telecomunicaciones de acuerdo con una de las reivindicaciones 9 a 13, caracterizado porque el número de identificación del aparato de telefonía móvil (60) es un Número IMSI (International Mobil Subscriber Identity), o un Número MSISDN (Mobil Subscriber ISDN).

15.- Sistema de telecomunicaciones de acuerdo con una de las reivindicaciones 9 a 14, caracterizado porque el servicio de autentificación (34), la aplicación de autentificación (61) del aparato de telefonía móvil (60) y la instalación de autentificación (21) del operador de la red de telefonía móvil (20) están configurados para la realización de una autentificación de acuerdo con 3GPP TS 33.223.

16.- Sistema de telecomunicaciones de acuerdo con una de las reivindicaciones 9 a 15, caracterizado porque el servicio de autentificación (34) y la plataforma (40) pertenecen al operador de telefonía móvil (20), en el que está anunciado el aparato de telefonía móvil (60), o a otro operador de telefonía móvil (150).

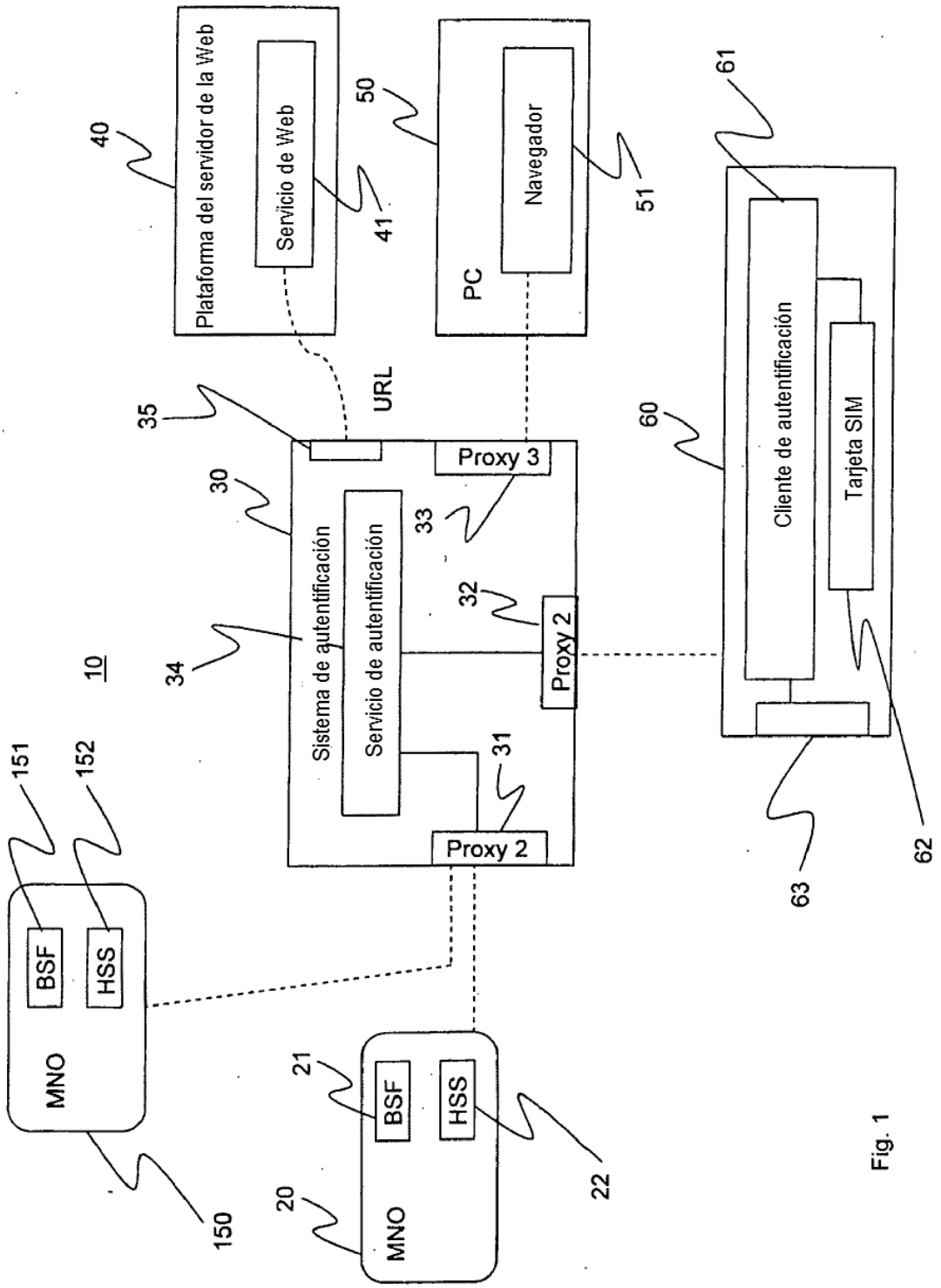
Plataforma del servidor de la Web
Servicio de Web
40
41
PC
Navegador
50
51
61
Cliente de autentificación
Tarjeta SIM
60
62
63
URL
35
Proxy 3
33
30
Sistema de autentificación
Servicio de autentificación
32
Proxy 2
34
10
31
Proxy 2
151
152
BSF
HSS
MNO
150
21
BSF
HSS
22
20
MNO

Fig. 1

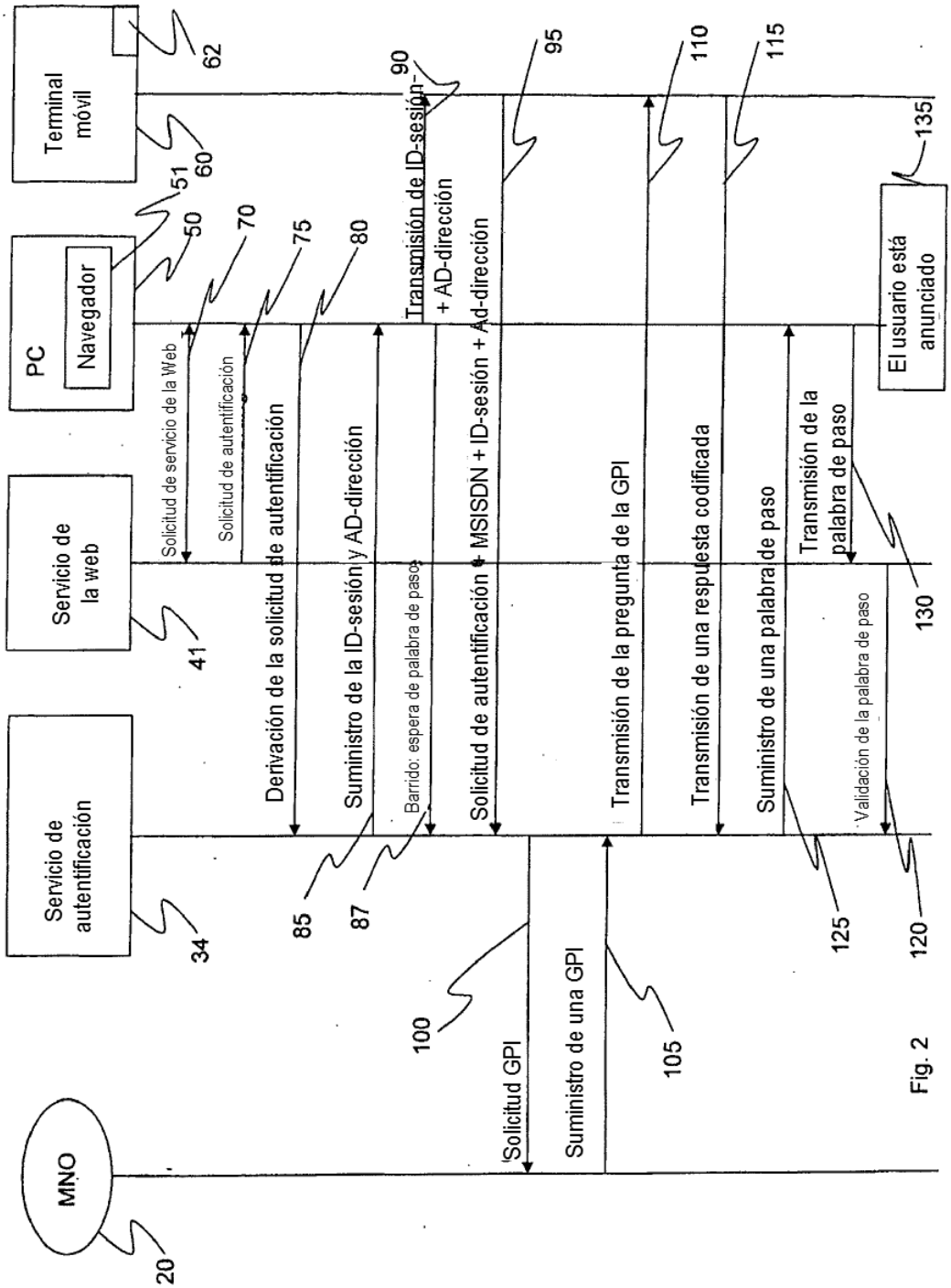
Terminal móvil
62
60
51
PC
Navegador
50
Servicio de la web
41
Servicio de autentificación
34
MNO
20
Solicitud de servicio de la Web
70
Solicitud de autentificación
75
Derivación de la solicitud de autentificación
80
Suministro de la ID-sesión y AD-dirección
85
Barrido: espera de palabra de paso
87
Transmisión de ID-sesión + AD-dirección
90
Solicitud de autentificación + MSISDN + ID-sesión + Ad-dirección
95
Solicitud GPI
100
Suministro de una GPI
105
Transmisión de la pregunta de la GPI
110
Transmisión de una respuesta codificada
115
Suministro de una palabra de paso
125
Transmisión de la palabra de paso
130
Validación de la palabra de paso
120
El usuario está anunciado
135

Fig. 2