(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 623 378**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
G06F 21/00 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.07.2011 PCT/EP2011/062641**

(87) Fecha y número de publicación internacional: **09.02.2012 WO12016858**

(96) Fecha de presentación y número de la solicitud europea: **22.07.2011 E 11740615 (7)**

(97) Fecha y número de publicación de la concesión europea: **01.02.2017 EP 2561662**

(54) Título: **Procedimiento y dispositivo para proporcionar una contraseña de un solo uso**

(30) Prioridad:

03.08.2010 DE 102010033232

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.07.2017

(73) Titular/es:

III HOLDINGS 12, LLC (100.0%)
2711 Centerville Road, Suite 400
Wilmington, DE 19808, US

(72) Inventor/es:

BUSSER, JENS-UWE y
FRIES, STEFFEN

(74) Agente/Representante:

MILTENYI, Peter

DESCRIPCIÓN

Procedimiento y dispositivo para proporcionar una contraseña de un solo uso

La invención se refiere a un procedimiento y un dispositivo para proporcionar una contraseña de un solo uso para un equipo de usuario para su registro en un servidor.

En muchos casos de aplicación, están conectados equipos de usuario a un servidor por medio de una red de datos insegura. Para que los equipos de usuario o equipos de cliente puedan intercambiar datos de forma segura con el servidor, los equipos de usuario son provistos en consecuencia con correspondientes credenciales de seguridad. Estas credenciales de seguridad, que pueden ser, por ejemplo, contraseñas u otros *tokens* de seguridad, son generados en muchos casos por un componente central, por ejemplo, un servidor de un proveedor de servicios, y después se distribuyen a los equipos de usuario o administradores de equipos de usuario o servicios de este tipo. En muchos casos, se emplean denominadas contraseñas de un solo uso (OTP - *One Time Passwort*). Con una contraseña de un solo uso OTP de este tipo, el equipo de usuario o del cliente puede registrarse una única vez en un servidor para un correspondiente servicio. Para futuros registros, el cliente debe establecer o bien una nueva contraseña o bien recibe del servidor un *token* de seguridad, por ejemplo, un certificado digital o un denominado *cookie*. Además, es posible que se utilicen otras contraseñas de un solo uso que, por ejemplo, se envíen previamente en una lista, por ejemplo, TANs o cadenas hash. Como contraseñas de un solo uso se usan por lo común secuencias aleatorias de caracteres. Tras generar una contraseña de un solo uso, la contraseña de un solo uso OTP se guarda en una base de datos. Si se registra un equipo de usuario o un cliente en el servidor, la contraseña de un solo uso (OTP) se marca como usada o se elimina de la base de datos. No es posible un segundo registro del equipo de usuario en el servidor con esta contraseña de un solo uso. Alternativamente es posible generar una cantidad suficiente de contraseñas de un solo uso conforme a un determinado procedimiento fijado y guardar solo las contraseñas de un solo uso ya utilizadas en la base de datos. Si se utilizan cadenas hash, en la base de datos se guarda solo, por ejemplo, la contraseña de un solo uso OTP utilizada por última vez. Por lo común, la contraseña de un solo uso OTP se guarda en páginas del servidor para posibilitar una comparación durante el registro del equipo de usuario en el servidor.

Otros ejemplos de contraseñas de un solo uso OTP convencionales son los denominados números de transacción TAN y números de transacción móviles TANs, que se utilizan, por ejemplo, en la banca *online*.

En contraseñas de un solo uso OTP convencionales, sin embargo, no es posible restringir o vincular a una determinada condición el uso de una contraseña de un solo uso OTP. Esto, sin embargo, es deseable en muchos casos, por ejemplo, cuando un usuario debe registrarse en el servidor desde un determinado equipo o cuando el registro del equipo de usuario en el servidor solo se puede efectuar en un determinado tiempo.

El documento US 2008 / 0 276 098 A1 desvela un sistema para proporcionar un acceso seguro para usuarios a un servidor desde equipos terminales inseguros.

El documento US 2007 / 0 079 135 A desvela un sistema para la autenticación de usuarios.

Por tanto, un objetivo de la presente invención es crear un procedimiento para proporcionar una contraseña de un solo uso para un equipo de usuario que ofrezca la posibilidad de vincular condiciones adicionales a la contraseña de un solo uso.

Este objetivo se logra de acuerdo con la invención por medio de un procedimiento con las características indicadas en la reivindicación 1 y de un servidor con las características indicadas en la reivindicación 10.

En una posible forma de realización del procedimiento de acuerdo con la invención, el identificador de uso unívoco es formado por un ID de usuario del usuario.

En otra posible forma de realización, el identificador de uso unívoco es formado por un ID de equipo de usuario del equipo de usuario.

En otra posible forma de realización del procedimiento de acuerdo con la invención, el identificador de uso unívoco es formado por una combinación del ID de usuario del usuario y del ID de equipo de usuario del equipo de usuario.

En una posible forma de realización del procedimiento de acuerdo con la invención, el servidor genera la contraseña de un solo uso calculando un valor de función criptográfico del identificador de uso unívoco.

En una posible forma de realización del procedimiento de acuerdo con la invención, el servidor calcula como contraseña de un solo uso (OTP) el valor de función criptográfico del identificador de uso por medio de una clave criptográfica secreta.

En una posible forma de realización del procedimiento de acuerdo con la invención, el servidor calcula como contraseña de un solo uso (OTP) el valor de función criptográfico por medio de una función criptográfica preestablecida, particularmente una función hash, para el identificador de uso unívoco de la clave criptográfica secreta.

En una posible forma de realización del procedimiento de acuerdo con la invención, el servidor calcula como contraseña de un solo uso (OTP) el valor de función criptográfico adicionalmente en función de una marca temporal.

En otra posible forma de realización del procedimiento de acuerdo con la invención, el servidor calcula como contraseña de un solo uso (OTP) el valor de función criptográfico adicionalmente en función de un número aleatorio.

En una posible forma de realización del procedimiento de acuerdo con la invención, el equipo de usuario guarda la contraseña de un solo uso (OTP) recibida del servidor y transmite esta contraseña de un solo uso (OTP) en un registro del equipo de usuario en el servidor junto con el identificador de uso.

En una posible forma de realización del procedimiento de acuerdo con la invención, el servidor verifica durante el registro del equipo de uso en el servidor el equipo de uso con ayuda del identificador de uso contenido implícitamente en la contraseña de un solo uso (OTP).

En una posible forma de realización del procedimiento de acuerdo con la invención, el servidor elimina la contraseña de un solo uso (OTP) generada por él tras la transmisión de la contraseña de un solo uso (OTP) generada al correspondiente equipo de usuario.

En una posible forma de realización del procedimiento de acuerdo con la invención, la contraseña de un solo uso (OTP) generada es enviada junto con el equipo de usuario al usuario para el registro del equipo de usuario del usuario en el servidor.

En una posible forma de realización del procedimiento de acuerdo con la invención, la contraseña de un solo uso (OTP) generada es enviada por el servidor por medio de una red de datos o por medio de un soporte de datos a un equipo de usuario instalado en la ubicación del usuario el usuario para su registro en el servidor.

En una posible forma de realización del procedimiento de acuerdo con la invención, la validez de la contraseña de un solo uso (OTP) generada por el servidor caduca tras un tiempo preestablecido.

En una posible forma de realización del servidor de acuerdo con la invención, el identificador de uso unívoco es formado por un ID de usuario de un usuario.

En una forma de realización alternativa del servidor de acuerdo con la invención, el identificador de uso unívoco es formado por un ID de equipo de usuario del equipo de usuario.

En una posible forma de realización del servidor de acuerdo con la invención, durante un registro del equipo de usuario en el servidor, el equipo de usuario se verifica con ayuda del identificador de uso contenido implícitamente en la contraseña de un solo uso recibida del servidor.

A continuación, se describe una posible forma de realización del procedimiento de acuerdo con la invención y del sistema de acuerdo con la invención para proporcionar una contraseña de un solo uso (OTP) haciendo referencia a la figura adjunta.

La figura 1 muestra un diagrama del proceso de señales para la aclaración del procedimiento de acuerdo con la invención y del servidor de acuerdo con la invención para proporcionar una contraseña de un solo uso.

Como se puede reconocer en la figura 1, un equipo de usuario 1 y un servidor 2 se comunican a través de una red de datos e intercambian mensajes. El equipo de usuario 1 puede ser cualquier equipo de usuario que esté instalado en la ubicación de un usuario, por ejemplo, en una casa. El equipo de usuario 1 puede ser un equipo de usuario móvil o instalado de manera fija. La red de datos puede ser una red de datos inalámbrica o por cable, así como un entramado de diferentes redes de datos como, por ejemplo, internet.

Un ejemplo de un equipo de usuario 1 es un *Energie Gateway* para una red de alimentación eléctrica inteligente. Otros ejemplos son equipos médicos que están instalados en el espacio de un paciente para el intercambio de datos de paciente con un correspondiente servidor de servicios. Otros posibles ejemplos son alarmas contra incendios o indicadores de alarma que entregan un aviso de alarma a un proveedor de servicios, por ejemplo, el cuerpo de bomberos. Además, el equipo de usuario 1 puede ser un aparato de comunicación, por ejemplo, un *TV-Box* de pago que posibilita a un usuario recibir películas de un servidor 2. El servidor 2, por ejemplo, puede encontrarse en las instalaciones de un proveedor de servicios o *serviceprovider*. El proveedor de servicios mismo o por encargo puede hacer fabricar equipos de uso 1 y entregarlos a posibles clientes. Alternativamente, los equipos de usuario 1 pueden adquirirse en el libre comercio. Los equipos de usuario 1 son en cada caso identificables de manera unívoca por medio de un número de serie o algo similar. Además, cada cliente o usuario puede poseer un número de cliente unívoco. Si un cliente que ha recibido un equipo de usuario 1 de un proveedor de servicios o lo ha comprado en el libre comercio desea registrar el equipo de usuario 1 en el proveedor de servicios, como se representa en la figura 1, envía un mensaje de solicitud o un *request* por medio de la red de datos al servidor 2 del proveedor de servicios. Con un generador previsto en el servidor 2, se genera posteriormente una contraseña de un solo uso OTP en una operación criptográfica en función de un identificador de uso unívoco. Un identificador de uso puede ser, por ejemplo, un ID de usuario del usuario, particularmente un número de cliente. Alternativamente, el identificador de uso

puede ser un ID de equipo de usuario, por ejemplo, un número de serie del equipo de usuario 1. Además, es posible que el identificador de uso sea una dirección unívoca como, por ejemplo, una dirección MAC. El servidor 2 transmite la contraseña de un solo uso OTP formada por medio de la operación criptográfica al equipo de usuario 1 que se ha de registrar por medio de la red de datos, como se representa en la figura 1.

La contraseña de un solo uso OTP generada puede transmitirse, como se representa en la figura 1, por medio de la red de datos al equipo de usuario 1, o también alternativamente por medio de otro canal de comunicación. Además es posible que la contraseña de un solo uso OTP generada se transmita por medio de un soporte de datos *offline* del servidor 2 al equipo de usuario 1. Este soporte de datos puede estar formado, por ejemplo, por una memoria USB. El soporte de datos, en una posible forma de realización, es enviado junto con el equipo de usuario 1 a instalar en un paquete por correo. El usuario conecta entonces al equipo de usuario 1 el soporte de datos adjunto, por ejemplo, una memoria USB, para la lectura de la contraseña de un solo uso OTP, de tal modo que el equipo de usuario 1 se puede registrar en el servidor 2 con ayuda de la contraseña de un solo uso OTP leída para la activación del servicio.

Además, es posible que el soporte de datos, por ejemplo, la memoria USB que transporta la contraseña de un solo uso OTP generada, sea enviada al usuario por separado del equipo de usuario 1 en otro paquete. En otra posible forma de realización, el soporte de datos es una memoria de datos integrada en el equipo de usuario 1. Esta memoria de datos, puede tener, por ejemplo, una protección de acceso y activarse con ayuda de una contraseña para que el usuario obtenga acceso a la contraseña de un solo uso OTP guardada en ella. Tan pronto como el usuario o el equipo de usuario 1 ha recibido *online* u *offline* la contraseña de un solo uso OTP formada por el servidor 2, el equipo de usuario 1 puede registrarse por medio de un mensaje de solicitud N en el servidor 2 para el correspondiente servicio. Con la contraseña de un solo uso OTP generada por el servidor 2 y recibida por el equipo de usuario 1, está contenido o codificado implícitamente en la contraseña de un solo uso OTP el identificador de uso, por ejemplo, una cuenta de usuario o un número de cliente o un correspondiente identificador de equipo, por ejemplo, un número de serie. De esta manera se impide que otro usuario u otro equipo se pueda registrar con esta contraseña de un solo uso OTP en el servidor 2. Si el servidor 2 forma, por ejemplo, la contraseña de un solo uso OTP para un equipo de usuario 1 por medio de una función hash a partir del ID de equipo conocido y una clave criptográfica secreta del ID de equipo, la contraseña de un solo uso OTP formada es unívoca: OTP = H (K_{priv}, ID de equipo). En este caso, también el ID de equipo del equipo de usuario 1 se envía al servidor 2 durante el registro, es decir, en el mensaje de registro N como parte del mensaje N. Después, el servidor 2, utilizando la clave criptográfica secreta (K_{priv}) puede comprobar eficientemente si la contraseña de un solo uso OTP es correcta sin que la contraseña de un solo uso OTP tenga que estar depositada centralmente en el servidor 2 para su comprobación. Debido a ello, en el procedimiento de acuerdo con la invención se da la posibilidad de que el servidor 2 borre o elimine de su memoria de datos la contraseña de un solo uso OTP generada por él tras la transmisión a los equipos de usuario 1. De esta manera, puede reducirse considerablemente el esfuerzo de administración por parte del servidor 2 o del proveedor de servicios. Además, esto ofrece la ventaja particular de que, en caso de un fallo de una memoria de datos por parte del servidor 2, incluso si se pierden este tipo de contraseñas de un solo uso OTP, puede efectuarse una verificación de la contraseña de un solo uso OTP recibida por parte del servidor 2.

En otra posible forma de realización, una validez de una contraseña de un solo uso OTP generada por el servidor 2 caduca tras un tiempo preestablecido configurable, por ejemplo, después de unos minutos u horas. Si el registro del equipo de usuario 1 es correcto, el servidor 2 puede comunicar esto al equipo de usuario 1 con un mensaje de OK.

En una posible forma de realización, en la transmisión del mensaje de registro N desde el equipo de usuario 1 al servidor 2, la contraseña de un solo uso OTP no se transmite en texto sin cifrar, sino con protección criptográfica. En otra posible forma de realización, la transmisión del mensaje N para el registro del equipo de usuario 1 en el servidor 2 se efectúa por medio de una conexión con protección criptográfica, por ejemplo, una conexión TLS o SSL. A este respecto, es posible que el mensaje de registro N transmitido se verifique con ayuda de una suma de comprobación.

En otra forma de realización preferente, el cálculo del valor de función criptográfico que forma la contraseña de un solo uso OTP se efectúa con una función criptográfica preestablecida, por ejemplo, una función hash, para el identificador de uso unívoco por medio de una clave criptográfica secreta usando informaciones o datos adicionales. A este respecto, el servidor 2, en una posible forma de realización, puede calcular como contraseña de un solo uso OTP el valor de función criptográfico adicionalmente en función de una marca temporal. Una indicación de tiempo o una marca temporal, por ejemplo, <MMAA> o <DDMMAA> o <días desde 01-01-2010>, hace posible que se genere una contraseña de un solo uso OTP adicional por cuenta de un usuario y por mes o día. Esta forma de realización es particularmente apropiada en caso de que una contraseña de un solo uso OTP sea válida solo brevemente y solo se requiera pocas veces una nueva contraseña de un solo uso. Además, es posible introducir en este lugar un denominado valor de tiempo UTC. Un *Unix Time* describe a este respecto, por ejemplo, el número de segundos transcurridos desde el 01-01-1970. De esta manera es posible, generar de manera muy rápida cambiantes contraseñas de un solo uso OTP para un determinado identificador de uso, por ejemplo: OTP=Hash(K, ID, <DDMMAA>).

Esta forma de realización puede utilizar una indicación de tiempo para crear o comprobar una contraseña de un solo uso OTP, debiendo estar disponible una indicación de tiempo sincronizada. En una posible forma de realización, se efectúa una sincronización de tiempo por medio de protocolos como, por ejemplo, NTP (*Network Time Protocol*) o IEEE 1588.

En otra posible forma de realización, el servidor envía como contraseña de un solo uso OTP un valor de función criptográfico adicionalmente en función de un número aleatorio. Este número aleatorio puede ser generado, por ejemplo, por medio de un generador aleatorio. Por ejemplo, la contraseña de un solo uso OTP se calcula de la siguiente manera:

OTP=Hash (K, <número aleatorio>, ID) | | <número aleatorio>

De esta manera, pueden generarse con números aleatorios correspondientemente largos tantas contraseñas de un solo uso OTP como se deseen.

En una variante especial, en lugar de un procedimiento hash en el que se concatena una clave K directamente con un mensaje, puede emplearse un denominado procedimiento HMAC. En una posible forma de realización, el valor HMAC se calcula como en el estándar RFC 2104:

HMAC (K, m) =H ((K XOR opad) | | H ((K XOR ipad) | | m))

siendo m un mensaje, por ejemplo, un mensaje de registro,

siendo opad e ipad *strings* predefinidos o cadenas de caracteres y

siendo K una contraseña de un solo uso OTP o un valor dependiente de la contraseña de un solo uso OTP, por ejemplo, K=H (OTP).

En otra posible variante de realización, en lugar de un procedimiento hash, también puede emplearse un algoritmo de cifrado simétrico, por ejemplo, AES (*Advanced Encryption Standard*) en un modo CBC-MAC (*Cipher Block Chaining Message Authentication Code*).

El procedimiento de acuerdo con la invención ofrece algunas ventajas. Con el procedimiento de acuerdo con la invención es posible crear una contraseña de un solo uso OTP conforme a una regla fija definida usando una operación criptográfica de tal manera que la contraseña de un solo uso OTP puede ser vinculada a un determinado identificador de uso, por ejemplo, un ID de usuario o un número de cuenta de usuario. Además, no es necesario guardar antes de su utilización la contraseña de un solo uso OTP en una memoria de datos del servidor 2, de tal modo que se facilita en su conjunto la administración de estos datos.

En una posible forma de realización, es posible ligar la contraseña de un solo uso OTP a un nombre de cliente de un usuario, por ejemplo, un cliente de una compañía eléctrica. Además, con el procedimiento de acuerdo con la invención es posible, en caso de requerirse, generar contraseñas de un solo uso OTP adicionales para el mismo usuario o para el mismo nombre de cliente. La contraseña de un solo uso OTP formada es criptográficamente tan segura como un número aleatorio puro. El creador o el servidor 2 de la contraseña de un solo uso OTP no tiene que guardar esta contraseña de un solo uso OTP formada. Por parte del servidor 2, solo es necesario guardar qué cuentas o equipos ya han utilizado sus contraseñas de un solo uso OTP o qué cuentas o equipos aún pueden utilizar sus contraseñas de un solo uso OTP. Esto reduce los datos que deben protegerse a la clave K criptográfica que se utiliza para crear las contraseñas de un solo uso OTP. Además, la validez de una contraseña de un solo uso OTP puede limitarse temporalmente. El procedimiento y sistema de acuerdo con la invención abre así a un proveedor de servicios o *serviceprovider* la posibilidad de vincular contraseñas de un solo uso OTP con determinadas condiciones y permite, por tanto, elevar la flexibilidad del proveedor de servicios y elevar la seguridad frente a manipulaciones.

REIVINDICACIONES

1. Procedimiento para proporcionar una contraseña de un solo uso (OTP) para un equipo de usuario (1) de un usuario, que está prevista para el registro del equipo de usuario (1) en un servidor (2),
en el que el servidor (2) genera la contraseña de un solo uso (OTP) por medio de una operación criptográfica en función de un identificador de usuario unívoco y transmitiéndola al equipo de usuario (1),
guardando el equipo de usuario (1) la contraseña de un solo uso (OTP) recibida del servidor (2) y transmitiéndola en un registro del equipo de usuario (1) en el servidor (2) junto con el identificador de uso,
verificando el servidor (2) durante el registro del equipo de usuario (1) en el servidor (2) el equipo de usuario (1) con ayuda del identificador de uso contenido implícitamente en la contraseña de un solo uso (OTP) recibida,
estando formado el identificador de uso unívoco por un ID de equipo de usuario del equipo de usuario (1).

2. Procedimiento de acuerdo con la reivindicación 1,
en el que el servidor (2) genera la contraseña de un solo uso (OTP) mediante cálculo de un valor de función criptográfico del identificador de uso.

3. Procedimiento de acuerdo con la reivindicación 2,
en el que el servidor (2) calcula como contraseña de un solo uso (OTP) el valor de función criptográfico del identificador de uso por medio de una clave criptográfica secreta (K_{priv}).

4. Procedimiento de acuerdo con la reivindicación 3,
en el que el servidor (2) calcula como contraseña de un solo uso (OTP) el valor de función criptográfico por medio de una función criptográfica preestablecida, particularmente una función hash, para el identificador de uso unívoco por medio de la clave criptográfica secreta.

5. Procedimiento de acuerdo con las reivindicaciones 2 a 4,
en el que el servidor (2) calcula como contraseña de un solo uso (OTP) el valor de función criptográfico adicionalmente en función de una marca temporal o un número aleatorio.

6. Procedimiento de acuerdo con las reivindicaciones 1 a 5,
en el que el servidor (2) elimina la contraseña de un solo uso (OTP) generada por él tras su transmisión al equipo de usuario (1).

7. Procedimiento de acuerdo con las reivindicaciones 1 a 6,
en el que se envía la contraseña de un solo uso (OTP) generada junto con el equipo de usuario (1) al usuario para el registro del equipo de usuario (1) del usuario en el servidor (2).

8. Procedimiento de acuerdo con las reivindicaciones 1 a 6,
en el que el servidor (2) envía la contraseña de un solo uso (OTP) generada por medio de una red de datos o por medio de un soporte de datos a un equipo de usuario (1) instalado en la ubicación del usuario para su registro en el servidor (2).

9. Procedimiento de acuerdo con las reivindicaciones 1 a 8,
en el que una validez de la contraseña de un solo uso (OTP) generada por el servidor (2) caduca después de un tiempo preestablecido.

10. Servidor (2) para proporcionar una contraseña de un solo uso (OTP) para un equipo de usuario (1) de un usuario, que está prevista para el registro del equipo de usuario (1) en el servidor (2),
en donde el servidor (2) genera la contraseña de un solo uso (OTP) por medio de una operación criptográfica en función de un identificador de uso unívoco y la transmite al equipo de usuario (1),
en donde el equipo de usuario (1) envía al servidor (2), para su registro en un servidor (2), la contraseña de un solo uso (OTP) recibida del servidor (2) junto con el identificador de uso, que, con ayuda del identificador de uso contenido implícitamente en la contraseña de un solo uso (OTP) y el identificador de uso recibido, verifica el equipo de usuario (1) y lo autoriza para un servicio;
estando formado el identificador de uso unívoco por un ID de equipo de usuario del equipo de usuario (1).

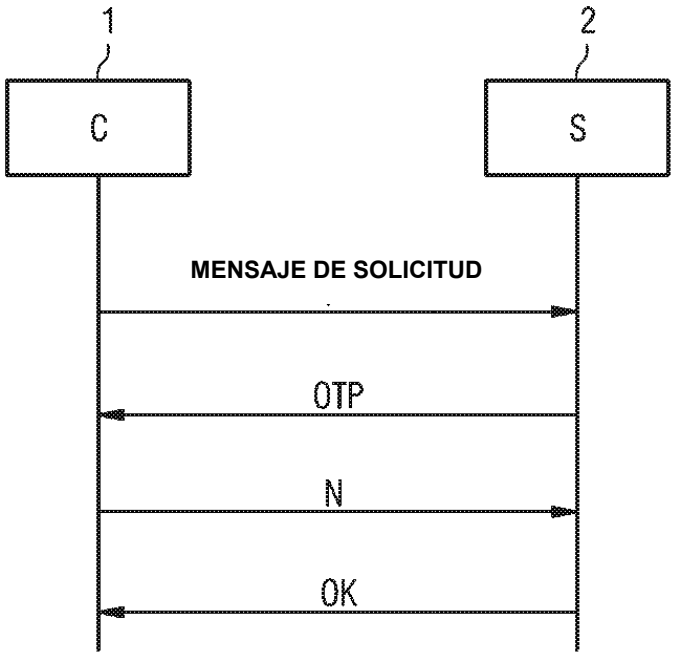

FIGURA 1