(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 935 717**

(51) Int. CI.:

G06F 21/31 (2013.01)
G06F 21/62 (2013.01)
H04L 9/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.03.2018 PCT/EP2018/056739**

(87) Fecha y número de publicación internacional: **20.09.2018 WO18167298**

(96) Fecha de presentación y número de la solicitud europea: **16.03.2018 E 18710883 (2)**

(97) Fecha y número de publicación de la concesión europea: **19.10.2022 EP 3566160**

(54) Título: **Método para autenticar un usuario y dispositivo, primer y segundo servidores y sistema correspondientes**

(30) Prioridad:

17.03.2017 EP 17305292

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.03.2023

(73) Titular/es:

THALES DIS FRANCE SAS (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

HUGOT, DIDIER

(74) Agente/Representante:

DEL VALLE VALIENTE, Sonia

DESCRIPCIÓN

Método para autenticar un usuario y dispositivo, primer y segundo servidores y sistema correspondientes

Campo de la invención

La invención se refiere generalmente a un método para autenticar un usuario.

Además, la invención pertenece a un dispositivo para autenticar un usuario.

La presente invención es particularmente aplicable a un campo de radiocomunicación móvil en donde el dispositivo es un terminal móvil, como, p. ej., un teléfono móvil.

Además, la invención también se refiere a un primer y un segundo servidores para autenticar un usuario.

Finalmente, la invención se refiere a un sistema para autenticar un usuario. El sistema incluye uno o varios dispositivos y dos o más servidores.

Estado de la técnica

El documento US-20050074126 A1 describe una técnica en la que un servidor de autenticación autentica un usuario de cliente. Para autenticar el usuario de cliente, el servidor compara una credencial recibida del cliente y que pertenece al usuario de cliente con las credenciales que pertenecen al usuario y almacenadas en un directorio. Cuando el servidor autentica satisfactoriamente el usuario, el servidor envía al cliente un tique que puede ser enviado y un tique de concesión de tiques (o TGT). El cliente envía el tique al servidor que redirige el tique a un servidor delegado y mantiene el TGT, como una cookie.

El documento US-20070044143 A1 describe una solución en la que un cliente usa servidores de autenticación para solicitar comunicación autenticada con un proveedor de servicios. El cliente envía al proveedor de servicios una solicitud de autenticación. La solicitud incluye su identificador único y un token de autenticación cifrado recibido de los servidores de autenticación. El token incluye el identificador único, una dirección de red y un nonce. Cada servidor de autenticación usó una clave dividida recibida del proveedor de servicios para cifrar y generar un token de autenticación parcial. El proveedor de servicios utiliza una clave secreta para descifrar el token de autenticación cifrado y obtener la información del token de autenticación. El proveedor de servicios utiliza la información del token de autenticación y el identificador único para decidir si la comunicación autenticada está autorizada.

Como se conoce per se, un usuario de un teléfono móvil ingresa sus credenciales de usuario para acceder a un servicio o servicios, como, p. ej., un servicio o servicios bancarios, gestionados por un servidor remoto. Por lo tanto, las credenciales de usuario se presentan al servidor que autentica satisfactoriamente el usuario cuando las credenciales de usuario presentadas coinciden con las credenciales de usuario de referencia.

Sin embargo, dicho servidor de autenticación tiene que registrar o acceder a las credenciales de usuario de referencia, para autenticar una pluralidad de usuarios.

Existe la necesidad de una solución alternativa mientras se autentica de forma segura usuarios en un lado del servidor.

Sumario de la invención

La invención propone una solución para satisfacer la necesidad especificada justo anteriormente en la presente memoria, proporcionando un método para autenticar un usuario.

En un primer aspecto de la invención, la invención define un método según la reivindicación 1.

El principio de la invención consiste en usar un primer servidor para identificar un usuario, para acceder a su credencial o credenciales de referencia y para generar un token o tokens de autenticación de referencia en base a la credencial o credenciales de usuario de referencia y una clave o claves predeterminadas. A continuación, el primer servidor transmite el token o tokens de autenticación de referencia a un segundo servidor identificado. El primer servidor instruye, a través del segundo servidor, a un usuario de dispositivo proporcionar su credencial o credenciales. El dispositivo genera un token o tokens de autenticación presentados en base a la credencial o credenciales de usuario proporcionadas y la clave o claves predeterminadas almacenadas por el dispositivo. A continuación, el dispositivo transmite al segundo servidor el token o tokens de autenticación presentados. El segundo servidor compara el token o tokens de autenticación presentados con respecto al token o tokens de autenticación de referencia recibidos. El segundo servidor transmite al primer servidor un resultado o resultados de comparación y/o un resultado de autenticación, como, p. ej., un estado relacionado con una autenticación de usuario satisfactoria o no satisfactoria, que se genera por el segundo servidor.

Solo el primer servidor accede a credenciales de usuario de referencia registradas y el segundo servidor solo procesa tokens, como datos cifrados que se originan tanto en el primer servidor como en el dispositivo de usuario, para autenticar (o no) un usuario registrado. Por lo tanto, el segundo servidor no procesa datos en texto simple, asegurando así el acceso a los datos procesados no revelando ni el usuario en cuestión ni su credencial o credenciales de referencia.

El primer y segundo servidores cooperan para autenticar, de manera segura, usuarios que son conocidos por el primer servidor sin necesidad de que el segundo servidor acceda ni a las identidades (o identificadores) de usuario en cuestión ni a sus credenciales de usuario de referencia asociadas.

Si una primera compañía gestiona el primer servidor mientras una segunda compañía gestiona el segundo servidor, entonces las identidades de usuario y las credenciales de usuario de referencia correspondientes no se conocen en el lado del segundo servidor. Por lo tanto, el segundo servidor mantiene una privacidad de los usuarios en cuestión que se identifican solo en el lado del primer servidor.

La solución reivindicada permite autenticar usuarios de manera segura sin necesidad de ningún acceso a las credenciales de usuario de referencia correspondientes del segundo servidor, como un servidor de autenticación (de tokens).

En el lado del dispositivo de usuario, los usuarios pueden usar sus credenciales de usuario asociadas habituales.

Por lo tanto, la solución de la invención es transparente para el usuario, manteniéndose al mismo tiempo la seguridad.

Por lo tanto, la solución de la invención permite acceder de manera segura a un servicio o servicios gestionados por o a través del primer servidor mientras se autentica de forma segura un usuario en cuestión a través del segundo servidor, como un servidor de autenticación.

También se describe, como ejemplo no limitativo, un dispositivo para autenticar un usuario.

El dispositivo está configurado para recibir de un segundo servidor al menos una solicitud para obtener al menos una credencial de usuario, obtener del usuario al menos una credencial de usuario presentada y generar y enviar al segundo servidor al menos un token de autenticación presentado. El al menos un token de autenticación presentado se genera en base a la al menos una credencial de usuario presentada y al menos una clave predeterminada. El dispositivo almacena la al menos una clave predeterminada.

El dispositivo puede ser un terminal de usuario, un elemento seguro (o SE) o cualquier tipo de dispositivo de comunicación.

En la presente descripción, un SE es un objeto inteligente que incluye un chip o chips que protegen, como un componente o componentes resistentes a la manipulación, el acceso a datos almacenados y que está destinado a comunicar datos con un dispositivo anfitrión de SE, como, p. ej., un teléfono móvil.

Según un segundo aspecto, la invención define un primer servidor para autenticar un usuario según la reivindicación 7.

El primer servidor está configurado para recibir de al menos un dispositivo al menos un identificador relacionado con un usuario, recuperar al menos una credencial de usuario de referencia asociada con el al menos un identificador de usuario, generar al menos un token de autenticación de referencia. El al menos un token de autenticación de referencia se genera en base a la al menos una credencial de usuario de referencia y al menos una clave predeterminada. El primer servidor está configurado para enviar a un segundo servidor (según un tercer aspecto) el al menos un token de autenticación de referencia y al menos un script para solicitar al usuario proporcionar al menos una credencial de usuario y recibir del segundo servidor al menos un resultado de comparación y/o un resultado de autenticación.

Un proveedor de servicios (u otro tercero) que opera el primer servidor, como un servidor de delegación de autenticación (de tokens), accede a las identidades (o identificadores) de usuario y las credenciales de usuario de referencia asociadas, mientras que es capaz de autenticar en cooperación con el segundo servidor los usuarios en cuestión.

Según un tercer aspecto, la invención define un segundo servidor para autenticar un usuario según la reivindicación 8.

El segundo servidor está configurado para recibir de un primer servidor (según el segundo aspecto) al menos un token de autenticación de referencia y al menos un script para solicitar al usuario proporcionar al menos una credencial de usuario. El segundo servidor está configurado para obtener al menos un identificador relacionado con un dispositivo a direccionar. El segundo servidor está configurado para enviar, en base al al menos un identificador relacionado con el dispositivo a direccionar, al dispositivo, al menos una solicitud para obtener al menos una credencial de usuario ejecutando el al menos un script para solicitar al usuario proporcionar al menos una credencial de usuario. El segundo servidor está configurado para recibir del dispositivo al menos un token de autenticación presentado. El segundo servidor está configurado para comparar cada uno del al menos un token de autenticación presentado con el token de autenticación de referencia recibido, generar al menos un resultado de comparación y/o un resultado de autenticación, y enviar al primer servidor el al menos un resultado de comparación y/o el resultado de autenticación.

Un proveedor de servicios (u otro tercero) que opera el segundo servidor, como un servidor de autenticación (de tokens), no necesita acceder a ninguna credencial de usuario de referencia, mientras que es capaz de autenticar en cooperación con el primer servidor usuarios desconocidos para el segundo servidor.

Según un cuarto aspecto, la invención define un sistema para autenticar un usuario según la reivindicación 9.

El sistema incluye al menos un dispositivo, un primer servidor y al menos un segundo servidor. El primer servidor está configurado para recibir del al menos un dispositivo al menos un identificador relacionado con un usuario, recuperar al menos una credencial de usuario de referencia asociada con el al menos un identificador de usuario, generar al menos un token de autenticación de referencia. El al menos un token de autenticación de referencia se genera en base a la al menos una credencial de usuario de referencia y al menos una clave predeterminada. El primer servidor está configurado para enviar a un segundo servidor el al menos un token de autenticación de referencia y al menos un script para solicitar al usuario proporcionar al menos una credencial de usuario. El segundo servidor está configurado para obtener al menos un identificador relacionado con un dispositivo a direccionar. El segundo servidor está configurado para enviar, en base al al menos un identificador relacionado con el dispositivo a direccionar, al dispositivo, al menos una solicitud para obtener al menos una credencial de usuario ejecutando el al menos un script para solicitar al usuario proporcionar al menos una credencial de usuario. El dispositivo está configurado para obtener del usuario al menos una credencial de usuario presentada, generar y enviar al segundo servidor al menos un token de autenticación presentado. El al menos un token de autenticación presentado se genera en base a la al menos una credencial de usuario presentada y la al menos una clave predeterminada. El dispositivo almacena la al menos una clave predeterminada. El segundo servidor está configurado para comparar cada uno del al menos un token de autenticación presentado con el token de autenticación de referencia recibido, generar al menos un resultado de comparación y/o un resultado de autenticación, y enviar al primer servidor el al menos un resultado de comparación y/o el resultado de autenticación.

Breve descripción de las figuras

Las características y ventajas adicionales de la invención resultarán más evidentes a partir de una descripción detallada de una realización preferida de la invención, dada como un ejemplo indicativo y no limitativo, junto con las siguientes figuras:

- La Figura 1 ilustra un diagrama simplificado de una realización de un sistema que comprende un equipo móvil, un primer y un segundo servidores, estando configurado el primer servidor para identificar un usuario, obtener una credencial o credenciales de usuario de referencia asociadas, emitir, a través del dispositivo, al segundo servidor, un token o tokens de autenticación de referencia correspondientes, y permitir, a través del segundo servidor, que el usuario presente una credencial o credenciales de usuario y el dispositivo emita un token o tokens de autenticación presentados correspondientes, estando adaptado el segundo servidor para comparar el token o tokens de autenticación presentados con el token o tokens de autenticación de referencia recibidos, respectivamente, según la invención; y

- la Figura 2 representa una realización de un flujo de mensajes entre el usuario, el teléfono, los servidores de la Figura 1, de modo que, además de una identificación de usuario y una recuperación de la credencial o credenciales de usuario de referencia correspondientes, el primer servidor emite, a través del dispositivo, al segundo servidor, un token o tokens de autenticación de referencia correspondientes que se compararán con un token o tokens generados por el dispositivo usando una credencial o credenciales de usuario presentadas, de modo que el primer servidor autentica (o no), según un resultado o resultados de comparación y/o autenticación emitidos por el segundo servidor, el usuario y el dispositivo.

Descripción detallada

A continuación en la presente memoria, se considera un caso en el que el método de la invención para autenticar un usuario se implementa mediante un terminal móvil que comprende o está acoplado o conectado a un SE, como un dispositivo para autenticar un usuario, y dos servidores remotos.

Según otra realización (no representada), el método de la invención para autenticar un usuario se implementa mediante un terminal móvil, como un dispositivo independiente para autenticar un usuario, y dos servidores. En otras palabras, el dispositivo no coopera con ningún otro dispositivo, como, p. ej., un SE, para generar notablemente un token o tokens de autenticación presentados en base a datos almacenados de manera segura dentro del dispositivo y datos proporcionados, como credenciales de usuario, por un usuario del dispositivo. Según una realización de este tipo, el dispositivo para autenticar un usuario está adaptado para realizar las funciones que se llevan a cabo por el SE y que se describen más adelante independientemente de un almacenamiento de datos seguro y una generación segura de un token o tokens de autenticación presentados.

El SE puede ser un chip incorporado, como, p. ej., una tarjeta de circuito integrado universal embebida (o eUICC) o una tarjeta de circuito integrado universal integrada (o iUICC), dentro de un terminal, como un dispositivo anfitrión de

SE, o un chip que está acoplado al terminal, como un dispositivo anfitrión de SE, e incluido dentro de una tarjeta inteligente (u otro medio). Por lo tanto, el chip puede estar fijado o ser extraíble con respecto a su dispositivo anfitrión.

La invención no impone ninguna limitación en cuanto a un tipo de tipo SE.

Como un SE extraíble, el mismo puede ser una tarjeta de tipo de módulo de identidad de abonado (o SIM), un módulo extraíble seguro (o SRM), una llave inteligente de tipo USB (acrónimo de "Bus Universal en Serie"), una (micro) tarjeta de tipo digital segura (o SD) o una tarjeta de tipo Multimedia (o MMC) o cualquier otro formato de tarjeta para acoplarse a un dispositivo anfitrión, como un dispositivo para autenticar un usuario.

Naturalmente, la realización descrita a continuación en la presente memoria solo es para ejemplificar los propósitos y no se considera que reduce el alcance de la invención.

La **Figura 1** muestra esquemáticamente un sistema 100 que incluye un equipo 10 de terminal (móvil) (o TE), un primer servidor (remoto) 162 y un segundo servidor (remoto) 164.

Los servidores primero 162 y segundo 164 son accesibles, a través del aire (o OTA), a través de Internet (o OTI) y/o a través de la nube (o OTC), a través de una red o redes de comunicación, como, p. ej., una red o redes de radiocomunicación móvil (no representadas), por una flota de dispositivos conectados, como, p. ej., el TE 10.

La red o redes de radiocomunicación móvil pueden incluir un Sistema Global para Comunicaciones Móviles (o GSM), un Servicio General de Paquetes de Radio (o GPRS), un Sistema Universal de Telecomunicaciones Móviles (o UMTS), un EDGE (acrónimo de "Velocidades de Datos Mejorados para la Evolución de GSM"), un Acceso Múltiple por División de Código (o CDMA) y/o una red o redes de tipo de Evolución a Largo Plazo (o LTE).

Un grupo de redes de radiocomunicación móvil de este tipo no es exhaustivo, sino solo ilustrativo.

Adicional o alternativamente, la red o redes de comunicación pueden incluir una WLAN (acrónimo para "red de área local inalámbrica") o una red de tipo Internet o Intranet, a la que se puede acceder a través de un enlace o enlaces de radiocomunicación de corto alcance (o SR), como, p. ej., Bluetooth, Wifi, Zigbee, un enlace o enlaces de tipo de comunicación de campo cercano (o NFC).

El TE 10 (móvil) (o no) incluye un teléfono 14 (móvil) y uno o varios chips dentro de un SE 12.

El chip o chips de SE están incorporados, posiblemente de manera extraíble, dentro de una placa de circuito impreso (o PCB) del teléfono 14, como un dispositivo anfitrión de chip.

El chip o chips también pueden incorporar al menos parte del componente o componentes, como, p. ej., un procesador de banda base, un procesador o procesadores de aplicaciones y/u otro componente o componentes electrónicos.

Alternativamente, el chip o chips incluyen un entorno de ejecución de confianza (o TEE), como un área segura de un procesador de teléfono (o terminal) y un entorno de tiempo de ejecución seguro.

El chip o chips se incluyen preferiblemente dentro del SE.

No obstante, el SE puede tener diferentes factores de forma.

En lugar de estar embebidos dentro de su dispositivo anfitrión, el chip o chips de SE pueden estar soportados en un medio, como una tarjeta inteligente o una llave, como, p. ej., una llave de tipo bus en serie universal (o USB), y están acoplados o conectados comunicativamente a su dispositivo anfitrión.

La invención no impone ninguna restricción en cuanto a un tipo de SE, cuando está presente.

Como SE extraíble, puede ser una llave inteligente del tipo USB, una (micro) tarjeta de tipo digital segura (o SD), una tarjeta de tipo Multimedia (o MMC), una tarjeta de tipo SIM o cualquier formato de tarjeta a acoplar a un dispositivo anfitrión de chip.

El SE 12 pertenece preferiblemente a un usuario, como un abonado a un servicio o servicios inalámbricos.

El SE 12 incluye uno o varios chips que comprenden un (micro) procesador o (micro) procesadores 122 (y/o un (micro) controlador o (micro) controladores), como medios de procesamiento de datos, una memoria o memorias 124, como medios de almacenamiento de datos, y una o varias interfaces 126 de entrada/salida (o E/S) que están todos en conexión interna, a través de un bus 123 de datos bidireccional interno, entre sí.

La interfaz o interfaces de E/S 126 permiten comunicar datos desde el chip o chips de SE internos al exterior del chip y a la inversa.

La memoria 124 almacena un sistema operativo (o SO).

En lugar de incluirse dentro del teléfono 14, el chip (de SE) es independiente mecánicamente del teléfono 14 y está incluido dentro de un medio. El medio (de chip) puede ser un reloj o un auricular, como un accesorio del teléfono 14. El medio puede ser cualquier otro dispositivo ponible, como, p. ej., una cámara, una vestimenta, una joya del usuario del teléfono o cualquier cosa que pueda acomodar o integrar el chip que el usuario 11 del teléfono lleva o a la que accede.

El SE 12 puede almacenar una identidad de equipo móvil internacional (o IMEI), un número de red digital de servicios integrados de abonado móvil (o MSISDN), una dirección de protocolo de Internet (o IP), una identidad de abonado móvil internacional (o IMSI) y/o una dirección o direcciones de correo electrónico, como un identificador o identificadores relacionados con el SE 12.

El SE 12 puede disponerse para recibir del primer servidor 162 uno o varios tokens de autenticación de referencia, uno o varios identificadores relacionados con un segundo servidor 164 y uno o varios scripts para solicitar al usuario proporcionar una o varias credenciales de usuario.

El SE 12 puede configurarse para enviar al segundo servidor identificado 164 el token o tokens de autenticación de referencia y el script o scripts para solicitar al usuario proporcionar una o varias credenciales de usuario.

El SE 12 está adaptado para recibir del segundo servidor 164 una o varias solicitudes para obtener una o varias credenciales de usuario, para obtener del usuario 11 (el SE 12 y/o el teléfono 14) una o varias credenciales de usuario proporcionadas (o presentadas).

El SE 12 recibe una clave o claves predeterminadas.

En lugar de recibir la clave o claves predeterminadas, el SE 12 es capaz de generarlas usando un algoritmo de generación de claves y datos secretos que son compartidos ambos con un servidor, como, p. ej., el primer servidor 162 o un servidor conectado al primer servidor 162.

El SE 12 almacena la clave o claves predeterminadas previamente recibidas o generadas a bordo.

La clave o claves predeterminadas pueden incluir una clave temporal predeterminada o una clave permanente para ser utilizada para generar un token o tokens de autenticación presentados correspondientes.

En lugar de una clave temporal predeterminada, el SE 12 puede usar una contraseña temporal, como, p. ej., una contraseña de un solo uso (u OTP), mediante el uso de un algoritmo de generación de contraseñas temporales y datos secretos que son compartidos ambos con un servidor, como, p. ej., el primer servidor 162 o un servidor conectado al primer servidor 162.

El token o tokens presentados así generados pueden ser un token o tokens temporales, como, p. ej., un token o tokens de un solo uso o un token o tokens permanentes.

Según una característica esencial de la invención, el SE 12 está adaptado para emitir uno o varios tokens (de autenticación) presentados en base a una o varias credenciales de usuario proporcionadas (o presentadas) y la clave o claves predeterminadas. Para generar el token o tokens presentados, el SE 12 almacena la clave o claves predeterminadas y un algoritmo de generación de tokens que se comparten ambos con un servidor, como, p. ej., el primer servidor 162 o un servidor conectado al primer servidor 162. Una vez generado, el SE 12 se configura para enviar al segundo servidor 164 el token o tokens presentados.

El SE 12 está conectado o acoplado al teléfono 14, como un terminal de usuario.

En lugar de un teléfono 14, el terminal de usuario puede ser un ordenador de sobremesa, un ordenador portátil, un reproductor multimedia, una consola de juegos, una tableta, un miniordenador portátil, un auricular y/o un asistente digital personal (o PDA) que incorpora un procesador o procesadores (de radio) de banda base o coopera con los mismos.

En lugar de un teléfono 14, el terminal de usuario puede ser cualquier otro dispositivo que incluye medios para procesar datos, que comprende o se conecta a medios de comunicación de radiofrecuencia (o RF) de largo alcance (o LR) y/o SR para intercambiar datos con el exterior, y que comprende o está conectado a medios para almacenar datos.

El teléfono 14, como terminal de usuario, se usa para acceder a los servidores primero 162 y segundo 164.

El teléfono 14 incluye uno o varios (micro) procesadores (y/o un (mico) controlador o (micro) controladores) (no representados), como medios para procesar datos, que comprenden y/o están conectados a una o varias memorias, como medios para almacenar datos, que comprenden o están conectados a medios para interactuar con un usuario,

como una interfaz máquina-hombre (o MMI), y que comprenden o están conectados a una antena 146 para intercambiar datos con el exterior.

La MMI del teléfono puede incluir una pantalla o pantallas 142 de visualización, un teclado o teclados 144, un altavoz y/o una cámara (no representada).

La MMI del teléfono se utiliza para presentar información a un usuario 11 del teléfono, como, p. ej., un mensaje para hacer que el usuario introduzca o proporcione datos, como una credencial o credenciales de usuario, y para obtener datos introducidos o proporcionados por el usuario.

La credencial o credenciales de usuario son conocidas y/o específicas solo para el usuario 11 del teléfono.

La MMI del teléfono permite que el usuario del teléfono interactúe con el teléfono 14.

Las memorias del teléfono pueden incluir una o varias EEPROM (acrónimo de "Memoria de Solo Lectura Programable Borrable Eléctricamente"), una o varias ROM (acrónimo de "Memoria de Solo Lectura"), una o varias memorias Flash, y/o cualquier otra memoria de diferentes tipos, como una o varias RAM (acrónimo de "Memoria de Acceso Aleatorio").

La antena 146 permite comunicar, a través de un enlace o enlaces 15 de RF, como uno o varios enlaces inalámbricos, a través de la red o redes de comunicación, datos con los servidores primero 162 y segundo 164.

La RF puede fijarse en varios cientos de MHz, p. ej., aproximadamente 850, 900, 1800, 1900 y/o 2100 MHz, tal como una RF de tipo LR.

Alternativa o adicionalmente a la RF de tipo LR, el teléfono 14 está conectado a o incluye medios de comunicación sin contacto (o CL) para intercambiar datos con el exterior, como, p. ej., a través de un punto de acceso Wifi (no representado), como un punto de acceso de red (o NAP), con los servidores primero 162 y segundo 164.

Dentro de la presente descripción, el adjetivo "CL" indica en particular que los medios de comunicación se comunican a través de uno o varios enlaces de RF de tipo SR.

El enlace o enlaces de RF de tipo SR pueden estar relacionados con cualquier tecnología CL que permita al teléfono 14 intercambiar datos, a través de un enlace de tipo CL, con los servidores primero 162 y segundo 164. La RF de SR puede estar relacionada, p. ej., con una tecnología o tecnologías de comunicación de tipo NFC, Wifi, Bluetooth y/o Bluetooth de baja energía (o BLE) o similares, como un canal o canales de (radio) comunicación no móvil.

El primer servidor 162 está conectado, a través del enlace o enlaces inalámbricos (bidireccionales) 15, al teléfono 14.

El primer servidor 162 puede ser operado por un operador de red móvil (o MNO), un operador de red virtual móvil (o MVNO), un operador bancario, un proveedor de servicios o en su nombre.

El primer servidor 162 se usa en cooperación con una flota de dispositivos (cliente), como, p. ej., el teléfono 14, y el segundo servidor 164, para autenticar (o no) los usuarios de dispositivo registrados preferiblemente solo en el lado del primer servidor 162.

El primer servidor 162 se identifica mediante un identificador de recursos uniforme (o URI), como, p. ej., un localizador de recursos uniforme (o URL), una dirección IP y/o similares, como un identificador o identificadores relacionados con el primer servidor 162. El identificador o identificadores del primer servidor pueden almacenarse dentro en el lado del dispositivo (ya sea la memoria del dispositivo o una memoria de SE incorporada o acoplada).

El primer servidor 162 está alojado por un ordenador que incluye medios de procesamiento de datos, como, p. ej., un procesador o procesadores (no representados), y una o varias interfaces de E/S para intercambiar datos con el exterior.

El primer servidor 162 incluye o está conectado a una memoria o memorias de primer servidor (no representadas), como medios de almacenamiento de datos, que almacenan una primera base de datos y uno o varios identificadores relacionados con un segundo servidor 164 para usarse como un servidor de autenticación de tokens.

La memoria de primer servidor almacena un URI, una URL, una dirección o direcciones IP y/o similares, como un identificador o identificadores relacionados con el segundo servidor 164 para participar para autenticar los usuarios registrados en el primer servidor 162.

El primer servidor 162 es capaz de acceder a la primera base de datos.

La primera base de datos registra preferiblemente datos relacionados con una pluralidad de abonados o cuentas de usuario, como datos relacionados con usuarios.

Cada cuenta de usuario se asocia con uno o varios identificadores relacionados con el usuario. La cuenta de usuario se puede asociar con una o varias IMSI, uno o varios URI, una o varias URL, una o varias direcciones de correo electrónico, una o varias direcciones IP, uno o varios MSISDN y/o similares, para identificar inequívocamente un dispositivo o dispositivos a direccionar y usar para autenticar el usuario.

El primer servidor 162 es capaz de recibir, para cada usuario (cliente), desde un dispositivo o dispositivos, uno o varios identificadores de usuario y/o uno o varios identificadores relacionados con un dispositivo o dispositivos a direccionar y usar para autenticar el usuario (en cuestión).

Los datos relacionados con los usuarios incluyen, para uno o varios identificadores relacionados con cada usuario registrado, una o varias credenciales de usuario de referencia.

La credencial o credenciales de usuario de referencia pueden incluir un número de identidad personal (o PIN) de referencia, una contraseña de referencia, una frase de contraseña de referencia, una contraseña de un solo uso (u OTP) de referencia y/o una o varias características biométricas de referencia, como, p. ej., una huella o huellas dactilares de referencia, una voz de referencia, un iris de referencia, una palma o palmas de referencia, una vena o venas de referencia y/o un reconocimiento o reconocimientos faciales de referencia relacionados con cada usuario en cuestión.

Para un usuario dado, uno o varios dispositivos de destino, como, p. ej., un teléfono, una tableta y/u otro dispositivo o dispositivos informáticos, como un terminal o terminales de usuario, en una asociación con uno o varios SE pueden registrarse dentro de la primera base de datos.

El primer servidor 162 (procesador) ejecuta preferiblemente una o varias funciones de seguridad, para proteger el acceso a la información gestionada a través de o mediante el primer servidor 162. Las funciones de seguridad incluyen preferiblemente un cifrado de datos usando una clave pública relacionada con el segundo servidor 164, para proteger el acceso a los datos cifrados en cuestión a enviar al segundo servidor 164. Las funciones de seguridad incluyen preferiblemente un descifrado de datos usando una clave privada relacionada con el primer servidor 162, para acceder a los datos descifrados en cuestión (en texto simple). Las funciones de seguridad incluyen preferiblemente una firma de datos usando una clave privada relacionada con el primer servidor 162, para demostrar que un originador de datos a enviar al segundo servidor 164 es el primer servidor 162.

El primer servidor 162 (procesador) está dedicado a ejecutar una aplicación de la invención para autenticar un usuario.

El primer servidor 162 desempeña una función de un servidor de delegación de autenticación de tokens (y no un servidor que delega una autenticación en base a credenciales de usuario de referencia).

El primer servidor 162 está adaptado para recibir de un dispositivo fuente, como, p. ej., el teléfono 14 o un ordenador de escritorio de usuario, un identificador o identificadores relacionados con un usuario (registrado).

El primer servidor 162 está configurado para recuperar en asociación con el usuario (identificado) una credencial o credenciales de usuario de referencia.

El primer servidor 162 puede configurarse para recuperar en asociación con el usuario un identificador o identificadores relacionados con un dispositivo o dispositivos de destino de referencia, como, p. ej. el teléfono 14. El dispositivo o dispositivos de destino de referencia pueden ser el dispositivo o dispositivos fuente (que proporcionan el identificador o identificadores de usuario) o distintos del dispositivo o dispositivos fuente.

Según una característica esencial de la invención, el primer servidor 162 está dispuesto para generar, en base a la credencial o credenciales de usuario de referencia y una clave o claves predeterminadas o una o varias OTP o una contraseña o contraseñas temporales, un token o tokens de (autenticación) de referencia, como datos cifrados relacionados con la credencial o credenciales de usuario de referencia.

Según una realización preferida, el primer servidor 162 está alojado en o conectado a un módulo de seguridad de hardware (o HSM). El HSM almacena la clave o claves predeterminadas (y otras claves) y proporciona, de manera segura, un servicio o servicios de procesamiento de cifrado, notablemente para generar un token o tokens de (autenticación) de referencia, en base a la clave o claves predeterminadas y un algoritmo de generación de tokens que almacena el HSM.

La clave o claves predeterminadas pueden incluir una clave temporal predeterminada o una clave permanente para ser utilizada para generar un token o tokens de referencia correspondientes.

En lugar de una clave temporal predeterminada, el primer servidor 162 puede usar una contraseña temporal, como, p. ej., una OTP, usando un algoritmo de generación de contraseñas temporales y datos secretos que son compartidos ambos con los dispositivos (cliente).

El token o tokens de referencia así generados pueden ser un token o tokens de referencia temporales, como, p. ej., un token o tokens de referencia de un solo uso, o un token o tokens de referencia permanentes.

El primer servidor 162 está adaptado preferiblemente para transmitir al dispositivo fuente o un dispositivo de destino (registrado) el token o tokens de referencia, uno o varios identificadores (registrados) relacionados con un segundo servidor 164 y uno o varios scripts para solicitar al usuario proporcionar o presentar una o varias credenciales de usuario. El script o scripts para solicitar al usuario proporcionar o presentar una o varias credenciales de usuario están destinados al segundo servidor 164 que es capaz de ejecutar dicho script o scripts. El script o scripts para solicitar al usuario proporcionar o presentar una o varias credenciales de usuario se predeterminan posiblemente en base a un motor de riesgo mientras se tiene en cuenta posiblemente el entorno de usuario (final), como, p. ej., el dispositivo de usuario, la ubicación del usuario, una naturaleza de la aplicación del dispositivo, como un navegador web o una aplicación móvil.

El primer servidor 162 está adaptado preferiblemente para recibir a través del dispositivo de usuario o directamente del segundo servidor registrado 164 un resultado de autenticación.

El primer servidor 162 está dispuesto para almacenar (o permitir almacenar) dentro de la memoria de primer servidor el resultado de autenticación.

El primer servidor 162 autoriza (cuando el usuario se ha autenticado satisfactoriamente) o prohíbe (cuando el usuario no se ha autenticado satisfactoriamente) el acceso a un servicio o servicios gestionados por el primer servidor 162 u otro servidor conectado al primer servidor 162.

El segundo servidor 164, como un servidor de autenticación (de tokens), puede ser operado por un proveedor de servicios o en su nombre.

El segundo servidor 164 está integrado dentro de una entidad de un sistema, como un sistema de extremo final.

El segundo servidor 164 está alojado por un ordenador que incluye medios de procesamiento de datos, como, p. ej., un procesador o procesadores (no representados), y una o varias interfaces de E/S para intercambiar datos con el exterior.

El segundo servidor 164 incluye o está conectado a una memoria o memorias de segundo servidor (no representadas), como medios de almacenamiento de datos, que almacenan una segunda base de datos.

El segundo servidor 164 es capaz de acceder a la segunda base de datos.

El segundo servidor 164 (procesador) ejecuta preferiblemente una o varias funciones de seguridad, para proteger el acceso a la información gestionada a través de o mediante el primer servidor 164. Las funciones de seguridad incluyen preferiblemente un cifrado de datos usando una clave pública relacionada con el primer servidor 162, para proteger el acceso a los datos así cifrados en cuestión. Las funciones de seguridad incluyen preferiblemente un descifrado de datos usando una clave privada relacionada con el segundo servidor 164. Las funciones de seguridad incluyen preferiblemente una firma de datos usando una clave privada relacionada con el segundo servidor 164, para demostrar que un originador de datos (a enviar) es el segundo servidor 164.

El segundo servidor 164 (procesador) está dedicado a ejecutar una aplicación de la invención para autenticar un usuario.

El segundo servidor 164 desempeña una función de un servidor de autenticación de tokens.

El segundo servidor 164 está adaptado preferiblemente para recibir de un dispositivo (fuente) o del primer servidor 162 un token o tokens (de autenticación) de referencia y uno o varios scripts para solicitar a un usuario proporcionar una o varias credenciales de usuario.

El segundo servidor 164 puede estar adaptado para recibir, de manera preferente del primer servidor 162, uno o varios identificadores relacionados con un dispositivo (de usuario) a direccionar y usar para autenticar el usuario en cuestión.

El segundo servidor 164 está configurado para registrar dentro de la segunda base de datos en asociación el token o tokens (de autenticación) de referencia (recibidos) y el script o scripts (recibidos) para solicitar al usuario proporcionar una o varias credenciales de usuario.

El segundo servidor 164 está adaptado para transmitir, en base al al menos un identificador relacionado con el dispositivo a direccionar, al dispositivo (de destino) una o varias solicitudes para obtener una o varias credenciales de usuario ejecutando el script o scripts para solicitar al usuario proporcionar una o varias credenciales de usuario. La ejecución, mediante el segundo servidor 164, del script o scripts para solicitar al usuario proporcionar una o varias credenciales de usuario crea un flujo de mensajes de autenticación que implica el dispositivo, el usuario y el segundo servidor 164. El flujo de mensajes de autenticación puede incluir, p. ej., una transmisión de una solicitud para obtener un PIN (o una contraseña) mediante el segundo servidor 164 al dispositivo seguido de una transmisión de una solicitud

para obtener una OTP (o una autenticación de tipo identidad rápida en línea (o FIDO), como, p. ej., una autenticación de característica biométrica) mediante el segundo servidor 164 al dispositivo.

El segundo servidor 164 está dispuesto preferiblemente para recibir del dispositivo uno o varios tokens (de autenticación) presentados.

Según una característica de la invención esencial, el segundo servidor 164 está configurado para comparar cada token presentado con un token de referencia (registrado) correspondiente. El segundo servidor 164 (u otro servidor conectado al segundo servidor 164) está configurado para analizar si el token presentado coincide o no con el token de referencia.

El segundo servidor 164 está adaptado para generar uno o varios resultados de comparación y/o un resultado de autenticación, es decir, un estado de autenticación de usuario satisfactorio o no satisfactorio. Solo si el token o tokens presentados coinciden con el token o tokens de referencia, el resultado de autenticación se establece en un estado de autenticación satisfactorio, como, p. ej., "válido". De lo contrario, es decir, si el token o tokens presentados no coinciden con el token o tokens de referencia, el resultado de autenticación se establece en un estado de autenticación no satisfactorio, como, p. ej., "no válido".

El segundo servidor 164 está dispuesto para almacenar (o permitir almacenar) dentro de la memoria de segundo servidor el resultado o resultados de comparación y/o el resultado de autenticación.

El segundo servidor 164 está configurado preferiblemente para enviar a través del dispositivo (fuente) o directamente al primer servidor 162 el resultado o resultados de comparación y/o el resultado de autenticación.

El segundo servidor 164 procesa anónimamente (es decir, sin conocer ningún identificador o identificadores de usuario) tokens de referencia o tokens presentados que se originan a partir de credenciales de usuario de referencia o credenciales de usuario presentadas, respectivamente.

La **Figura 2** representa una realización ilustrativa de un flujo 20 de mensajes que implica el usuario 11, el TE 10, como un dispositivo de usuario, el primer servidor 162, como un servidor de delegación de autenticación de tokens, y el segundo servidor 164, como un servidor de autenticación de tokens.

En el ejemplo descrito, se asume que el usuario 11 de TE ha utilizado un navegador web soportado por el teléfono 14 para solicitar acceso al primer servidor 162. A continuación, el primer servidor 162 solicita al usuario 11 de TE que se identifique, para conectarse al primer servidor 162. Se asume además que el usuario 11 de TE está registrado en el lado del primer servidor 162 y tiene una o dos credenciales de usuario de referencia, como, p. ej., una contraseña o una contraseña y una OTP, para autenticarse. Además, se asume asimismo que el primer servidor 162 y el segundo servidor 164 intercambian a través del TE 10, como el dispositivo de usuario. Según una alternativa (no representada), el primer y el segundo servidores intercambian directamente, es decir, sin pasar a través del dispositivo de usuario.

Inicialmente, el segundo servidor 164 establece un resultado (de autenticación) intermedio y un resultado (de autenticación) final a "1".

El usuario 11 de TE introduce, como un identificador de usuario, un nombre de usuario o una dirección de correo electrónico usando, p. ej., la MMI del teléfono.

Alternativa o adicionalmente, el usuario 11 de TE ingresa un MSISDN relacionado con su teléfono 14 y/o una IMSI, como un identificador o identificadores de dispositivo de usuario, usando, p. ej., la MMI del teléfono.

Se asume que el TE 10 intercambia con el primer servidor 162 usando, p. ej., mensajes de tipo de protocolo de transferencia de hipertexto (o HTTP) o HTTP seguro (o HTTPS). Sin embargo, cualquier otro protocolo de comunicación de datos entre el TE 10 y el primer servidor 162 puede usarse alternativa o adicionalmente con respecto al protocolo de tipo HTTP(S).

Una vez que el usuario 11 de TE ha proporcionado uno o varios identificadores de usuario, el TE 10 envía al primer servidor 162 un mensaje 22 que incluye una solicitud para obtener acceso a un servicio gestionado por el primer servidor 162 que incluye o está acompañado de la dirección de correo electrónico, como el identificador o identificadores de usuario, y/o el MSISDN y/o IMSI, como el identificador o identificadores de dispositivo de usuario.

El mensaje 22 incluye preferiblemente un URL predeterminada relacionada con el primer servidor 162, como un primer identificador de servidor particular.

El primer servidor 162 puede verificar (no representado) si el usuario identificado está o no autorizado a acceder a un servicio solicitado de este modo. Si el primer servidor 162 identifica que el usuario 11 no está autorizado a acceder al servicio, entonces el primer servidor 162 deniega el acceso al servicio y aborta un proceso de transacción iniciado.

Por lo tanto, no se realiza la transacción. De lo contrario, es decir, solo si el primer servidor 162 identifica que el usuario 11 está autorizado a acceder al servicio, el primer servidor 162 continúa un proceso de transacción iniciado.

El primer servidor 162 obtiene 24, p. ej., una contraseña de referencia, como la credencial o credenciales de usuario de referencia, que está asociada con el identificador o identificadores de usuario registrado.

Opcionalmente, el primer servidor 162 genera 26 una clave que se usa solo una vez o un número limitado de veces, como una clave temporal, o de manera permanente, como una clave permanente usando un algoritmo de generación de claves y datos secretos compartidos con el TE 10, como un dispositivo de usuario registrado.

En lugar de una generación de una clave temporal (o permanente), el primer servidor 162 genera 26 una OTP, como una contraseña que se usa solo una vez, o un número limitado de veces, como una contraseña temporal, mediante el uso de un algoritmo de generación de OTP (o contraseña temporal) y datos secretos compartidos con el TE 10.

El primer servidor 162 accede a la clave temporal (o permanente) predeterminada.

El primer servidor 162 genera 28 uno (o varios) tokens de autenticación de referencia en base a, p. ej., la contraseña de referencia, como la credencial o credenciales de usuario de referencia, y la clave predeterminada (o la OTP predeterminada o la contraseña temporal predeterminada).

Opcionalmente, antes de enviar el token o tokens de autenticación de referencia, el primer servidor 162 cifra el token o tokens de autenticación de referencia usando una clave pública relacionada con el segundo servidor 164 y/o firma el token o tokens de autenticación de referencia usando una clave privada relacionada con el primer servidor 162.

El primer servidor 162 envía al TE 10 un mensaje 210 que incluye el token o tokens de autenticación de referencia (posiblemente cifrados), una URL relacionada con el segundo servidor 164 y un script o scripts para solicitar al usuario proporcionar una (o varias) credenciales de usuario.

Opcionalmente, el mensaje 210 u otro mensaje separado (no representado) incluye además la clave o claves predeterminadas que se han cifrado preferiblemente mediante el primer servidor 162 usando una clave pública relacionada con el TE 10 (el teléfono 14 o el SE 12) y/o firmado usando una clave privada relacionada con el primer servidor 162.

La clave o claves predeterminadas son únicas y válidas para el token o tokens de autenticación de referencia y el token o tokens de autenticación presentados o distintas entre sí y cada una de las claves predeterminadas es válida para solo uno de los tokens de autenticación de referencia y solo uno de los tokens de autenticación presentados.

A continuación, el TE 10 envía al segundo servidor (identificado) 164 un mensaje 212 que incluye el token de autenticación de referencia (posiblemente cifrado) y el script o scripts para solicitar al usuario proporcionar una (o varias) credenciales de usuario.

Según una alternativa (no representada), en lugar de los dos últimos mensajes 210 y 212, el primer servidor 162 envía directamente (en lugar de pasar a través del TE 10) al segundo servidor 164 un mensaje único que incluye el token o tokens de autenticación de referencia (posiblemente cifrados) y un script o scripts para solicitar al usuario proporcionar una (o varias) credenciales de usuario. Adicionalmente, o bien en el mismo mensaje o bien en un mensaje separado, el primer servidor 162 envía directamente al segundo servidor 164 preferiblemente el MSISDN y/o el IMSI, como un identificador o identificadores relacionados con el TE 10, para identificar el TE 10, como el dispositivo a direccionar y usar para autenticar el usuario.

El segundo servidor 164 obtiene el identificador o identificadores del TE 10, recibiendo del TE 10 (o el primer servidor 162) el identificador o identificadores del TE 10.

Después de un posible descifrado de datos y/o una posible verificación de firma (satisfactoria), el segundo servidor 164 almacena (no representado) el token de autenticación de referencia (recibido) y el script o scripts (recibidos) para solicitar al usuario proporcionar una (o varias) credenciales de usuario.

Al ejecutar 214 el script (recibido) para solicitar al usuario proporcionar una credencial de usuario, el segundo servidor 164 envía, en base al MSISDN y/o IMSI, al TE 10 un mensaje 216 que incluye una solicitud para obtener del usuario 11 una credencial de usuario.

El usuario 11 introduce o proporciona una credencial de usuario presentada.

El TE 10 recibe del usuario 11 una contraseña presentada 218, como una credencial de usuario presentada.

Opcionalmente, el TE 10 genera (no representado) una clave que o bien se usa solo una vez o bien un número limitado de veces, como una clave temporal, o de manera permanente, como una clave permanente usando el algoritmo de generación de claves y los datos secretos compartidos con el primer servidor 162.

En lugar de una generación de una clave temporal (o permanente), el TE 10 genera 220 una OTP, como una contraseña que se usa solo una vez, o un número limitado de veces, como una contraseña temporal, mediante el uso del algoritmo de generación de OTP (o la contraseña temporal) y los datos secretos compartidos con el primer servidor 162.

El TE 10 accede a la clave predeterminada (temporal o permanente), ya sea generada previamente a bordo o recibida del primer servidor 162.

El TE 10 genera 222 un token de autenticación presentado en base a la contraseña presentada, como la credencial de usuario presentada, y la clave predeterminada (o la OTP o la contraseña temporal).

Una vez se genera, el TE 10 envía al segundo servidor 164 un mensaje 224 que incluye el token de autenticación presentado.

Después de un posible descifrado de datos y/o una posible verificación de firma (satisfactoria), el segundo servidor 164 almacena (no representado) el token de autenticación presentado.

El segundo servidor 164 compara 226 cada autenticación presentada (recibida del TE 10) con un token de autenticación de referencia correspondiente (recibido a través del TE 10 (o directamente) del primer servidor 162).

El segundo servidor 164 genera 228 un resultado de comparación, es decir, una coincidencia (de tokens) satisfactoria o no satisfactoria, como, p. ej., un "1" para una coincidencia satisfactoria o un "0" para una coincidencia no satisfactoria.

El segundo servidor 164 almacena (no representado) el resultado de comparación.

El segundo servidor 164 verifica 230 si existe o no otra acción, es decir, otro script para solicitar al usuario proporcionar, p. ej., una OTP, como otra credencial de usuario, a ejecutar.

Si existe otro script para solicitar al usuario proporcionar otra credencial de usuario a ejecutar, entonces el segundo servidor 164 genera 232 un resultado intermedio en base al resultado de comparación generado previamente y el valor de resultado intermedio anterior, es decir, el resultado intermedio establecido por primera vez. Para generar el resultado intermedio, el segundo servidor 164 multiplica el resultado de comparación generado previamente por el valor de resultado intermedio anterior. Por lo tanto, tan pronto como un resultado de comparación es no satisfactorio, el resultado intermedio pasa a ser "0". El segundo servidor 164 almacena el resultado intermedio. A continuación, el segundo servidor 164 repite para cada otro script:

- una ejecución 214 de script con otro script para solicitar al usuario proporcionar, p. ej., una OTP, como otra credencial de usuario;
- una transmisión 216 de script con una solicitud al usuario de proporcionar, p. ej., una OTP;
- una recepción 218 del usuario 11 de una OTP presentada;
- una generación 222 de un token de autenticación presentado correspondiente;
- una transmisión del token 224 de autenticación presentado;
- una comparación 226 del token de autenticación presentado con un token de autenticación de referencia (recibido);
- una generación 228 de un resultado de comparación;
- una verificación 230 de una existencia de una acción adicional, es decir, un script adicional, a ejecutar; y (cuando solo existen dos scripts)
- una generación 234 de un resultado final, como un resultado de autenticación.

De lo contrario, es decir, cuando no existe otro script para solicitar al usuario proporcionar otra credencial de usuario a ejecutar, el segundo servidor 164 genera 234 un resultado final, en base al resultado de comparación generado anterior y el valor de resultado final anterior, es decir, el resultado final establecido por primera vez. Para generar el resultado final, como un resultado de autenticación, el segundo servidor 164 multiplica el resultado de comparación generado previamente por el valor de resultado final anterior. El resultado de autenticación constituye un estado de autenticación satisfactorio o no satisfactorio, como, p. ej., un "1" o "0" respectivamente. El segundo servidor 164 almacena el resultado de autenticación.

Opcionalmente, antes de enviar datos, como, p. ej., el resultado o resultados de comparación y/o el resultado de autenticación, el segundo servidor 164 cifra los datos usando una clave pública relacionada con el primer servidor 162 y/o firma los datos usando una clave privada relacionada con el segundo servidor 164.

El segundo servidor 164 envía al TE 10 un mensaje 236 que incluye el resultado de autenticación (posiblemente cifrado) (y/o el resultado o resultados de comparación (posiblemente cifrados)).

El TE 10 envía al primer servidor 162 un mensaje 238 que incluye el resultado de autenticación (posiblemente cifrado) (y/o el resultado o resultados de comparación (posiblemente cifrados)).

Según una alternativa (no representada), en lugar de los dos últimos mensajes 236 y 238, el segundo servidor 164 envía directamente (en lugar de pasar a través del TE 10) al primer servidor 162 un único mensaje que incluye el resultado de autenticación (posiblemente cifrado) (y/o el resultado o resultados de comparación (posiblemente cifrados)).

La solución de la invención permite delegar una autenticación de usuario de un primer servidor que accede a una credencial o credenciales de usuario para cada usuario registrado a un segundo servidor transmitiendo (a través de un dispositivo de usuario) al segundo servidor un token de autenticación correspondiente sin necesidad de afectar a la experiencia de usuario (ya que el usuario aún puede usar su credencial o credenciales de usuario habituales).

La solución de la invención permite llevar a cabo una operación de autenticación de usuario segura mientras implica un dispositivo de usuario y al menos dos servidores en cooperación en base a una “tokenización” sobre la marcha de una credencial o credenciales de usuario registradas y accesibles solo por el primer servidor y una autenticación de tokens por el segundo servidor (sin ninguna “des-tokenización”).

REIVINDICACIONES

1. Un método para autenticar un usuario, que comprende:
recibir (162), mediante un primer servidor, de al menos un dispositivo, al menos un identificador (22) relacionado con un usuario;

- recuperar (24), mediante el primer servidor, al menos una credencial de usuario de referencia asociada con el al menos un identificador de usuario;
- generar (28), mediante el primer servidor, al menos un token de autenticación de referencia, siendo generado el al menos un token de autenticación de referencia en base a la al menos una credencial de usuario de referencia y al menos una clave predeterminada;
- enviar, mediante el primer servidor, a un segundo servidor, al menos un identificador relacionado con un dispositivo a direccionar, el al menos un token de autenticación de referencia y al menos un script para solicitar al usuario proporcionar al menos una credencial de usuario (210 y 212);
- enviar, mediante el segundo servidor, al dispositivo, al menos una solicitud (216) para obtener al menos una credencial de usuario ejecutando (214) el al menos un script para solicitar al usuario proporcionar al menos una credencial de usuario;
- obtener (218), mediante el dispositivo, del usuario, al menos una credencial de usuario presentada;
- generar (222) y enviar (224), mediante el dispositivo, al segundo servidor, al menos un token de autenticación presentado, siendo generado el al menos un token de autenticación presentado en base a la al menos una credencial de usuario presentada y la al menos una clave predeterminada, almacenando el dispositivo la al menos una clave predeterminada;
- comparar (226), mediante el segundo servidor, cada uno del al menos un token de autenticación presentado con el token de autenticación de referencia recibido y genera al menos un resultado de comparación y/o un resultado de autenticación;
- enviar, mediante el segundo servidor, al primer servidor, el al menos un resultado de comparación y/o el resultado de autenticación (236 y 238).

2. Método según la reivindicación 1, en donde, antes de generar el al menos un token de autenticación de referencia, el primer servidor genera (26) y envía (210) al dispositivo la al menos una clave predeterminada.

3. Método según la reivindicación 1, en donde, antes de generar el al menos un token de autenticación de referencia, el primer servidor genera la al menos una clave predeterminada usando un algoritmo de generación de claves y datos secretos, siendo compartidos el algoritmo de generación de claves y los datos secretos con el dispositivo y, antes de generar el al menos un token de autenticación presentado, el dispositivo genera la al menos una clave predeterminada usando el algoritmo de generación de claves y los datos secretos.

4. Método según cualquiera de las reivindicaciones 1 a 3, en donde, antes de enviar el al menos un token de autenticación de referencia, el primer servidor cifra el al menos un token de autenticación de referencia usando una clave pública relacionada con el segundo servidor y/o firma el al menos un token de autenticación de referencia usando una clave privada relacionada con el primer servidor y/o, antes de enviar el al menos un token de autenticación presentado, el dispositivo cifra el al menos un token de autenticación presentado usando una clave pública relacionada con el segundo servidor y/o firma el al menos un token de autenticación presentado usando una clave privada relacionada con el dispositivo.

5. Método según cualquiera de las reivindicaciones 1 a 4, en donde, antes de enviar el al menos un resultado de comparación y/o el resultado de autenticación, el segundo servidor cifra el al menos un resultado de comparación y/o el resultado de autenticación usando una clave pública relacionada con el primer servidor y/o firma el al menos un resultado de comparación y/o el resultado de autenticación usando una clave privada relacionada con el segundo servidor.

6. Método según cualquiera de las reivindicaciones 1 a 5, en donde la al menos una clave predeterminada es única y válida para el al menos un token de autenticación de referencia y el al menos un token de autenticación presentado o la al menos una clave predeterminada es distinta entre sí y cada una de la al menos una clave predeterminada es válida para solo uno del al menos un token de autenticación de referencia y solo uno del al menos un token de autenticación presentado.

7. Un primer servidor (162) para autenticar un usuario,
en donde el primer servidor está configurado para:

- recibir (22), de al menos un dispositivo, al menos un identificador relacionado con un usuario;
- recuperar (24) al menos una credencial de usuario de referencia asociada con el al menos un identificador de usuario;
- generar (28) al menos un token de autenticación de referencia, siendo generado el al menos un token de autenticación de referencia en base a la al menos una credencial de usuario de referencia y al menos una clave predeterminada;

- enviar, a un segundo servidor según la reivindicación 8, al menos un identificador relacionado con un dispositivo a direccionar, el al menos un token de autenticación de referencia y al menos un script para solicitar al usuario proporcionar al menos una credencial de usuario (210 y 212); y
- recibir, del segundo servidor, al menos un resultado de comparación y/o un resultado de autenticación (236 y 238).

8. Un segundo servidor (164) para autenticar un usuario,
en donde el segundo servidor está configurado para:

- recibir, de un primer servidor según la reivindicación 7, al menos un identificador relacionado con un dispositivo a direccionar, al menos un token de autenticación de referencia y al menos un script para solicitar al usuario proporcionar al menos una credencial de usuario (224);
- enviar, al dispositivo (10), al menos una solicitud (216) para obtener al menos una credencial de usuario ejecutando (214) el al menos un script para solicitar al usuario proporcionar al menos una credencial de usuario;
- recibir, del dispositivo, al menos un token de autenticación presentado (224);
- comparar (226) cada uno del al menos un token de autenticación presentado con el token de autenticación de referencia recibido;
- generar (228) al menos un resultado de comparación y/o un resultado de autenticación; y
- enviar, al primer servidor, el al menos un resultado de comparación y/o el resultado de autenticación (236 y 238).

9. Un sistema (100) para autenticar un usuario,

en donde el sistema incluye al menos un dispositivo (10), un primer servidor (162) y al menos un segundo servidor (164), el primer servidor está configurado para:

- recibir, del al menos un dispositivo, al menos un identificador relacionado con un usuario (22);
- recuperar (24) al menos una credencial de usuario de referencia asociada con el al menos un identificador de usuario;
- generar (28) al menos un token de autenticación de referencia, siendo generado el al menos un token de autenticación de referencia en base a la al menos una credencial de usuario de referencia y al menos una clave predeterminada;
- enviar, a un segundo servidor, al menos un identificador relacionado con un dispositivo a direccionar, el al menos un token de autenticación de referencia y al menos un script para solicitar al usuario proporcionar al menos una credencial de usuario (210 y 212);

en donde el segundo servidor está configurado para enviar, al dispositivo, al menos una solicitud (216) para obtener al menos una credencial de usuario ejecutando (214) el al menos un script para solicitar al usuario proporcionar al menos una credencial de usuario;
en donde el dispositivo está configurado para:

- obtener (218), del usuario, al menos una credencial de usuario presentada;
- generar (222) y enviar, al segundo servidor, al menos un token de autenticación presentado (224), siendo generado el al menos un token de autenticación presentado en base a la al menos una credencial de usuario presentada y la al menos una clave predeterminada, almacenando el dispositivo la al menos una clave predeterminada;

en donde el segundo servidor está configurado para:

- comparar (226) cada uno del al menos un token de autenticación presentado con el token de autenticación de referencia recibido;
- generar al menos un resultado de comparación (228) y/o un resultado de autenticación (234); y
- enviar, al primer servidor, el al menos un resultado de comparación y/o el resultado de autenticación (236 y 238).

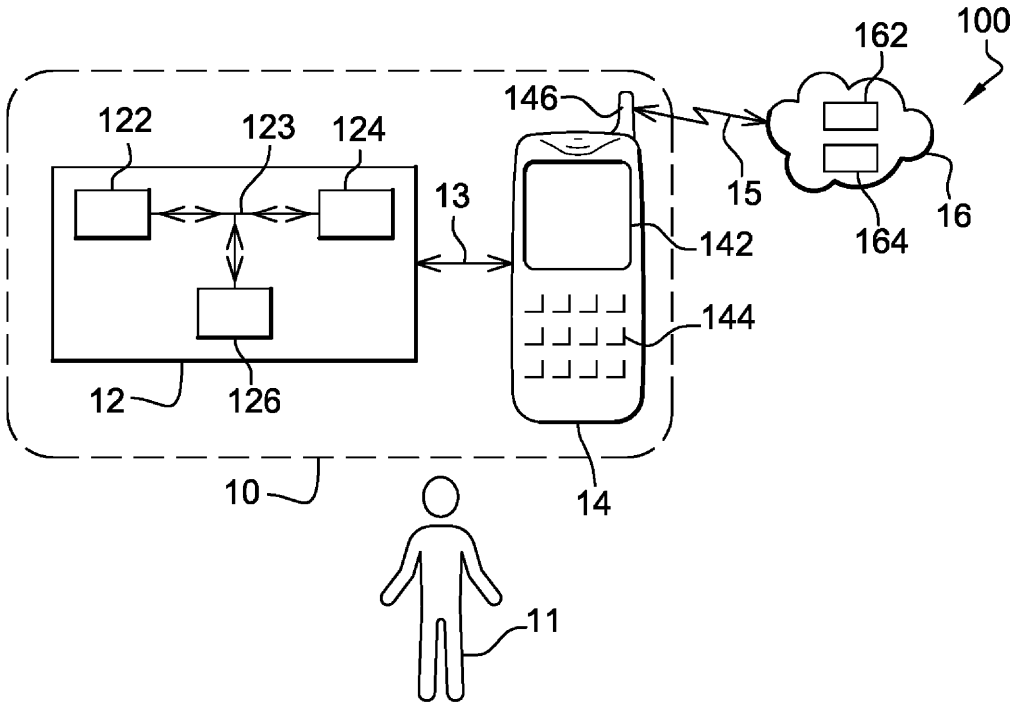

Fig. 1

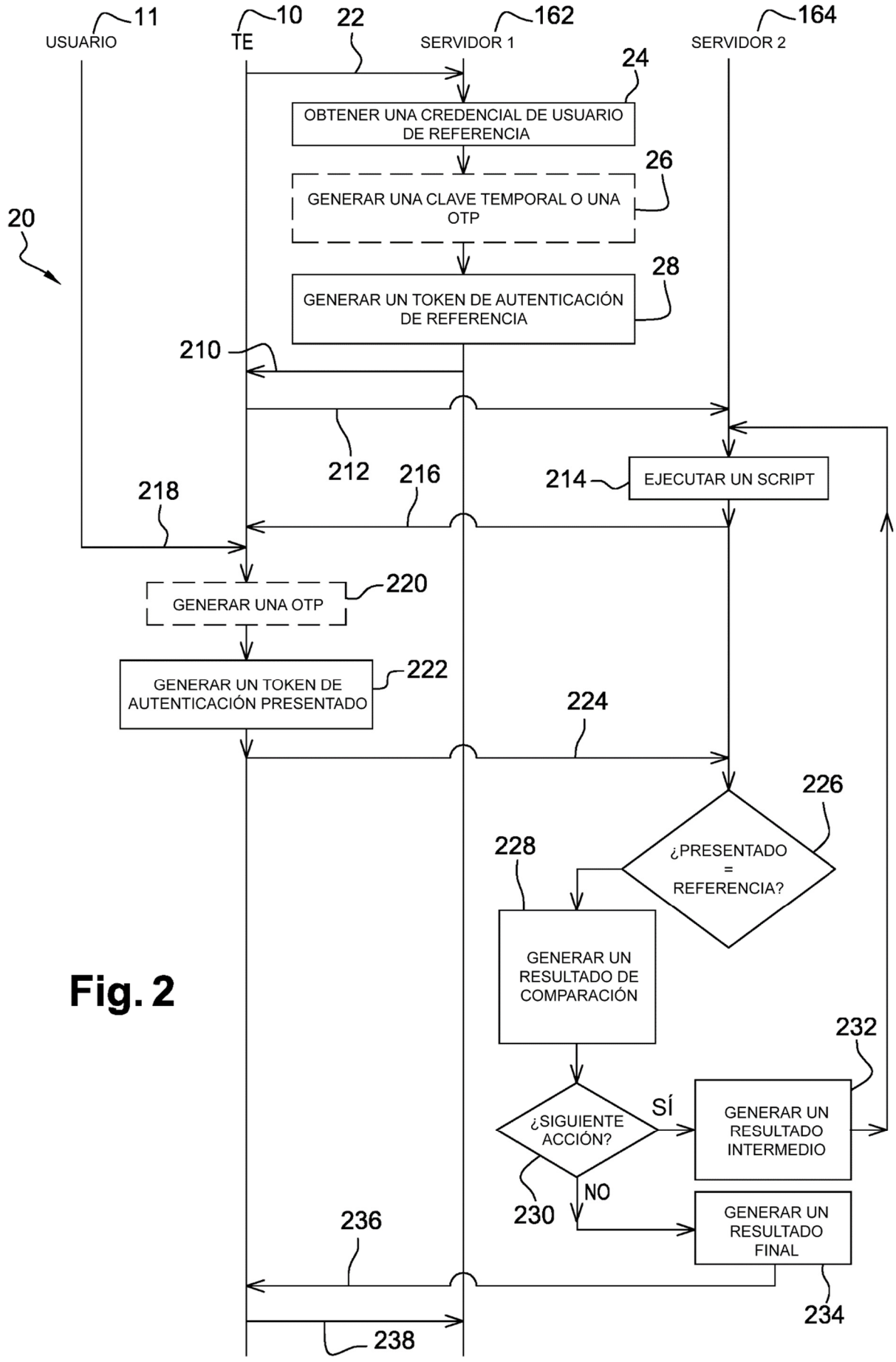
11
USUARIO
10
TE
22
162
SERVIDOR 1
164
SERVIDOR 2
24
OBTENER UNA CREDENCIAL DE USUARIO DE REFERENCIA
26
GENERAR UNA CLAVE TEMPORAL O UNA OTP
20
28
GENERAR UN TOKEN DE AUTENTICACIÓN DE REFERENCIA
210
212
216
214
EJECUTAR UN SCRIPT
218
220
GENERAR UNA OTP
222
GENERAR UN TOKEN DE AUTENTICACIÓN PRESENTADO
224
226
¿PRESENTADO = REFERENCIA?
228
GENERAR UN RESULTADO DE COMPARACIÓN
232
¿SIGUIENTE ACCIÓN?
SÍ
GENERAR UN RESULTADO INTERMEDIO
230
NO
GENERAR UN RESULTADO FINAL
234
236
238

Fig. 2