(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 380 320**

(51) Int. CI.:

G06F 21/20 (2006.01)
H04L 29/06 (2006.01)
H04L 12/56 (2006.01)
H04W 84/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03778346 .1**
(96) Fecha de presentación: **07.11.2003**
(97) Número de publicación de la solicitud: **1680720**
(97) Fecha de publicación de la solicitud: **19.07.2006**

(54) Título: **Procedimiento y sistema para la autenticación de un usuario de un sistema de procesado de datos**

(45) Fecha de publicación de la mención BOPI:
10.05.2012

(45) Fecha de la publicación del folleto de la patente:
10.05.2012

(73) Titular/es:
TELECOM ITALIA S.P.A.
PIAZZA DEGLI AFFARI, 2
20123 MILANO, IT

(72) Inventor/es:
SENTINELLI, Mauro

(74) Agente/Representante:
Ponti Sales, Adelaida

DESCRIPCIÓN

Procedimiento y sistema para la autenticación de un usuario de un sistema de procesado de datos

[0001] La presente invención se refiere en general al campo de los sistemas de procesamiento de datos, y, de manera más específica, a unos procedimientos para autenticar usuarios de sistemas de procesamiento de datos.

[0002] Hoy en día, la autenticación (es decir, verificación de la identidad) de usuarios de sistemas de procesamiento de datos con el fin de concederles el derecho a acceder a servicios predeterminados es un problema particularmente experimentado.

[0003] Para los fines de la presente descripción, el término servicio debe ser considerado de manera amplia, para incluir cualquier servicio posible que un sistema de procesamiento de datos puede ofrecer a un usuario, incluyendo la simple conexión a una computadora y/o a una red de computadoras, la conexión a la intranet de una compañía, una administración pública, una agencia gubernamental y/o a la Internet, acceso a un servicio de mensajería electrónica, acceso a un sitio Web que ofrece, por ejemplo, servicios de banca remota (inspección de cuentas y/o colocación de disposiciones), acceso a bases de datos y así sucesivamente (ésta es meramente una lista limitada y no exhaustiva de lo que se quiere decir por servicio en el contexto de la presente descripción).

[0004] En particular, una autenticación segura de los usuarios que solicitan acceso a servicios específicos ofrecidos por un sistema de procesamiento de datos es importante siempre que estos servicios involucren poner a la disposición de los usuarios información confidencial, tal como, por ejemplo, el contenido de buzones de mensajería electrónica, o información personal relacionada por ejemplo con la salud de individuos, o proyectos de investigación de una compañía, sólo por citar unos pocos ejemplos.

[0005] El problema de autenticar usuarios no es solamente encontrado en tales sistemas de procesamiento de datos a gran escala tales como la Internet (la cual, como se sabe, a pesar de su éxito impresionante, es extremadamente insegura), sino también a una escala más pequeña, tal como en infraestructuras de procesamiento de datos de compañías medianas o incluso pequeñas, en donde el acceso a servicios particulares tales como las bases de datos de nómina de empleados, los registros de contabilidad y similares debe ser concedido a los usuarios de manera selectiva.

[0006] Diversos procedimientos de autenticación han sido propuestos. Probablemente la solución de autenticación más ampliamente adoptada se basa en condicionar el acceso a servicios predeterminados a la provisión por el usuario de un código de identificación personal, típicamente un par formado por nombre de usuario y clave.

[0007] Esta técnica, también conocida como autenticación estática basada en clave, es extremadamente insegura, por ejemplo debido a que los usuarios, preocupados de que olvidarán el nombre de usuario y la clave que les fueron asignados, pueden escribirlos por ejemplo en un papel, haciendo que estos códigos de identificación personal, que deberían ser más bien mantenidos estrictamente en secreto, sean potencialmente accesibles a otras personas; adicionalmente, el nombre de usuario y la clave usualmente viajan a través del sistema de procesamiento de datos sin codificación, y así pueden ser obtenidos de manera más o menos fraudulenta por otras personas, que escuchan el tráfico de datos.

[0008] Un procedimiento de autenticación mejorado es descrito en la US 6.230.002 B1, que se relaciona con la autenticación de anfitriones inalámbricos asociados con terminales móviles del Sistema Global para Comunicaciones Móviles (GSM por sus siglas en inglés). En este procedimiento, una clave es generada por un Módulo de Identificación de Suscriptor (SIM por sus siglas en inglés) de un terminal móvil de GSM acoplado al anfitrión inalámbrico, y la clave generada es comunicada (a través de la red de GSM) a un servidor de autenticación de una red privada para obtener acceso a un sitio protegido de la misma.

[0009] Algunos de los procedimientos de autenticación propuestos más recientemente se derivan de la extensión de los sistemas de comunicaciones telefónicas móviles, especialmente el GSM.

[0010] En todos los procedimientos de esta clase, se usa para la autenticación el SIM que cada teléfono móvil incluye y que almacena información sobre el suscriptor del servicio de comunicaciones telefónicas móviles, particularmente datos usados para permitir que el teléfono móvil obtenga acceso a la red de GSM.

[0011] Éste es el caso, por ejemplo, del procedimiento y el sistema de autenticación descritos en la solicitud internacional Nº WO 00/02406, en la cual un usuario de una red de comunicaciones de Protocolo de Internet (IP por sus siglas en inglés) (tal como la Internet), que desea conectarse con la red de IP a través de su terminal de red de IP (por ejemplo, un Asistente Digital Personal, PDA por sus siglas en inglés), usa el mismo SIM (o uno esencialmente similar) que es usado en su teléfono móvil de GSM para autenticación en la red de IP, de ese modo el procedimiento de autenticación de una red de GSM existente es utilizado para autenticación en la red de IP.

[0012] Otros procedimientos de autenticación conocidos usan un canal de comunicación seguro, autenticado por SIM, formado por una red telefónica de GSM para distribuir claves a usuarios, usando entonces las claves recibidas, por ejemplo, en su teléfono móvil personal para tener acceso a servicios proporcionados a través de un canal no seguro tal como la Internet.

[0013] Un ejemplo de este tipo de procedimiento es proporcionado en la Publicación de Solicitud de Patente de EE.UU. 2003/0061503 A1, que describe un procedimiento de autenticación de acuerdo con el cual, cuando un dispositivo no autenticable que corresponde a un usuario solicita un servicio a través de un enlace inseguro tal como la Internet, o una Red de Área Local (LAN por sus siglas en inglés) o una LAN Inalámbrica, durante la conexión al servicio el usuario identifica un enlace seguro asociado con el mismo, proporcionando el número de teléfono móvil personal. El teléfono móvil del usuario es entonces contactado, y una clave (que preferentemente puede ser usada sólo una vez) le es comunicada; al introducir la clave a través del dispositivo no autenticable, el usuario es autorizado a acceder al servicio.

[0014] El Solicitante observa que los procedimientos de autenticación conocidos en el arte, aunque son satisfactorios bajo muchos aspectos, sin embargo no garantizan un nivel suficiente de seguridad de autenticación.

[0015] En particular, en sistemas tales como aquellos de acuerdo con los primeros dos ejemplos descritos anteriormente, el SIM que es usado para autenticar al usuario propuesto de los servicios del sistema de procesamiento de datos puede perderse o ser sustraído de manera fraudulenta de su legítimo propietario, y personas no autorizadas pueden así obtener acceso a los servicios de operación restringida.

[0016] Algo similar puede ocurrir en sistemas que se basan en la distribución de claves a través de la red de GSM: también en este caso, el terminal de GSM, o incluso solamente el SIM usado para autenticar el terminal de GSM del usuario en la red de GSM, puede perderse o ser sustraído de manera fraudulenta, y de ese modo personas no autorizadas pueden obtener acceso a los servicios de uso restringido.

[0017] En US 2003/0051041 se describe un procedimiento y aparato para la integración de funciones de facturación y de autenticación en redes de datos inalámbricas de área local y amplia. Un pórtico de facturación / autorización convergente (CBG) permite a un operador de WAN inalámbrica proporcionar un servicio de acceso a LAN a sus suscriptores WAN existentes. El esquema de autenticación se divide en tres grandes categorías. La primera categoría y la tercera se han diseñado para terminales sin soporte de SIM. La segunda categoría está diseñada para terminales con soporte SIM: la tarjeta SIM en el terminal se utiliza para proporcionar autenticación, una suscripción durante el servicio, así como el uso del servicio.

[0018] En US 2002/0097876 se describe un procedimiento de comunicación que comprende un dispositivo de comunicación personal que comprende una memoria en la que se almacena un número secreto, y un dispositivo digital capaz de comunicación con el dispositivo de comunicación personal. El procedimiento comprende las etapas de establecer la comunicación entre el dispositivo de comunicación personal y el dispositivo digital, proporcionando el número secreto del dispositivo de comunicación personal para el dispositivo digital.

[0019] El Solicitante siente que un grado de seguridad superior a aquél que puede ser logrado operando las técnicas de autenticación conocidas sería conveniente. Por lo tanto, un objeto de la presente invención es mejorar la seguridad de los procedimientos de autenticación conocidos.

[0020] El Solicitante ha encontrado que un procedimiento de autenticación que involucra la operación de dos módulos de identificación de suscriptor permite lograr un nivel muy elevado de seguridad.

[0021] En particular, el Solicitante ha encontrado que el nivel de seguridad es sumamente aumentado si se proporciona un procedimiento de autenticación que comprende dos fases de autenticación, a saber, una autenticación basada en SIM de un terminal de procesamiento de datos del usuario que solicita acceso a los servicios restringidos, y una segunda fase de verificación de la identidad del usuario, llevada a cabo operando una red de comunicación segura, tal como una red de comunicación móvil.

[0022] Para los fines de la presente invención, por autenticación basada en SIM se quiere decir cualquier autenticación que involucre un intercambio de datos de identificación almacenados en un Módulo de Identidad de Suscriptor.

[0023] De acuerdo con un primer aspecto de la presente invención, se propone un procedimiento como se expone en la reivindicación 1 anexa para autenticar un terminal de procesamiento de datos de un usuario con el fin de conceder acceso del terminal de procesamiento de datos a servicios seleccionados proporcionados por un sistema de procesamiento de datos, el usuario estando provisto de un terminal de comunicación móvil autenticable adaptado para ser usado en una red de comunicación móvil.

[0024] De acuerdo con otro aspecto de la presente invención, se proporciona un método como se expone en la reivindicación 3 mediante el cual un terminal de procesamiento de datos en un sistema de procesamiento de datos se autentica con el fin de tener acceso a los servicios seleccionados proporcionados por el sistema de procesamiento de datos.

[0025] De acuerdo con todavía otro aspecto de la presente invención, se proporciona un sistema como en la reivindicación 5 para autenticar un terminal de procesamiento de datos de un usuario a fin de conceder el acceso al terminal procesamiento de datos a los servicios seleccionados proporcionados por un sistema de procesamiento de datos.

[0026] De acuerdo con todavía otro aspecto de la presente invención, se proporciona un kit de autenticación segura como se establece en la reivindicación anexa 21, para autenticar un terminal de procesamiento de datos de un usuario en un sistema de procesamiento de datos a fin de conceder el acceso al terminal procesamiento de datos a los servicios seleccionados proporcionados por un sistema de procesamiento de datos.

[0027] Las características y ventajas de la presente invención se harán evidentes a partir de la siguiente descripción detallada de algunas realizaciones de la misma, proporcionadas meramente a modo de ejemplos no limitativos, descripción que será conducida haciendo referencia a los dibujos anexos, en los cuales:

- la Figura 1 muestra gráficamente un ejemplo de sistema de procesamiento de datos en el cual un procedimiento de autenticación segura de usuario de acuerdo con una realización de la presente invención es activado de manera ventajosa;

- la Figura 2 muestra esquemáticamente, en términos de bloques funcionales pertinentes para el entendimiento de la realización citada de la invención, un servidor de autenticación y un operador de red de GSM;

- la Figura 3 muestra esquemáticamente, en términos de bloques funcionales, un contenido de una memoria de trabajo de una computadora de usuario durante una fase de autenticación llevada a cabo activando el procedimiento de autenticación segura de acuerdo con la realización citada de la invención; y

- la Figura 4 muestra esquemáticamente, en términos de diagramas de flujo simplificados, la operación de los diferentes elementos que cooperan para implementar el procedimiento de autenticación segura de acuerdo con la realización citada de la invención.

[0028] Con referencia a los dibujos, un escenario puramente a modo de ejemplo y no limitativo en absoluto, en el cual un procedimiento de autenticación segura de usuario de acuerdo con una realización de la presente invención puede ser activado, es mostrado gráficamente en la Figura 1. Un sistema de procesamiento de datos distribuidos, identificado globalmente por el número de referencia 100, comprende una red de computadoras local privada 105, por ejemplo una Red de Área Local (LAN por sus siglas en inglés), particularmente pero no limitativamente una red de Ethernet, una Red de Área Metropolitana (MAN por sus siglas en inglés) o una Red de Área Amplia (WAN por sus siglas en inglés), que constituye la infraestructura de computación de una entidad, por ejemplo una empresa o una agencia de administración pública; el tipo específico de red de computadora local 105 es totalmente irrelevante para los fines de la presente invención.

[0029] En términos extremadamente generales, la red de computadoras local privada 105 comprende una o más computadoras de servidor, tales como la computadora de servidor 110 mostrada en el dibujo, que proporcionan servicios específicos a una pluralidad de computadoras de clientes, tales como las computadoras de clientes 115a y 115b mostradas en el dibujo, las diferentes computadoras estando conectadas a una infraestructura de comunicación de datos 120 por la cual las diferentes computadoras pueden comunicarse entre sí. La potencia de procesamiento de las diferentes computadoras de la red local privada 105 puede variar sustancialmente: las computadoras de clientes 115a, 115b de la red son por ejemplo computadoras personales, particularmente computadoras móviles tales como computadoras portátiles, o estaciones de trabajo, operadas por el personal de la entidad, por ejemplo los empleados, para llevar a cabo sus deberes respectivos; la computadora de servidor 110 puede ser una computadora personal configurada convenientemente, una estación de trabajo o incluso una computadora grande y rápida que realiza varios trabajos a la vez. Los servicios proporcionados por la computadora de servidor 110 a las computadoras de clientes 115a, 115b pueden incluir almacenamiento de archivos electrónicos (servidor de archivos), servicios de aplicación de software (servidor de aplicaciones), servicios de manejo de bases de datos (servidor de base de datos), servicios de mensajería electrónica (correo electrónico) (servidor de correo), y cualquier otro servicio posible; aunque el tipo específico de servicios proporcionados por dichas una o más computadoras de servidor de la red local privada 105 no es pertinente para la presente invención, a continuación, sólo a modo de ejemplo, se asumirá que la computadora de servidor 110 actúa por lo menos como un servidor de correo para la red local privada 105.

[0030] La red local privada 105 también comprende una compuerta 125, por ejemplo un módem/encaminador de Red Digital de Servicios Integrados (ISDN por sus siglas en inglés) o de Línea de Suscriptor Digital (XDSL por sus siglas en inglés), que conecta en interfaz la red local privada 105 con un punto de acceso 130a a una red de computación externa 135; a continuación se asumirá que la red de computación externa 135 es una red abierta, particularmente la Internet (y así una red intrínsecamente insegura), aunque esto no debe ser considerado como limitativo para la presente invención; el punto de acceso 130a es así, por ejemplo, un Proveedor de Servicios de conectividad a Internet (ISP por sus siglas en inglés).

[0031] Una computadora de usuario remoto 140, por ejemplo una computadora portátil, está también conectada (puede ser conectada) a la Internet 135 a través de un punto de acceso 130b, el cual puede coincidir con el punto de acceso (ISP) 130a o, de manera más general, puede ser un punto de acceso diferente, localizado en un área geográfica diferente, o los dos puntos de acceso 130a y 130b pueden ser Puntos de Presencia (POP por sus siglas en inglés) diferentes de un mismo ISP. Con este fin, la computadora 140 opera por ejemplo un módem (por ejemplo, un módem de ISDN) y una conexión de marcado, o un módem de XDSL y una conexión de XDSL al punto de acceso 130b, o una conexión de LAN Inalámbrica (WLAN por sus siglas en inglés) al punto de acceso 130b (tal como una conexión de Fidelidad Inalámbrica, WI-FI por sus siglas en inglés, un tipo de acceso a Internet que se está haciendo popular en áreas tales como hoteles y aeropuertos).

[0032] Un usuario remoto USERa de la computadora 140 es por ejemplo un empleado del dueño de la empresa de la red local privada 105, que desea tener acceso a la red local privada 105 de su patrono y aprovechar los servicios proporcionados por una o más computadoras de servidor 110 de la misma desde un lugar remoto, es decir, sin estar conectado a la red local 105 directamente, sino a través de la red (abierta) externa 135; éste puede ser el caso, por ejemplo, de un empleado que está fuera de la oficina por negocios o incluso de vacaciones, y que desea tener acceso al servidor de correo 110 de la empresa para revisar su buzón de correo personal para buscar nuevos mensajes urgentes posibles.

[0033] Se asume que, con el fin de tener acceso a la red local privada 105, particularmente el servidor de correo 110, el usuario remoto necesita que lo autentiquen, de modo a evitar accesos fraudulentos a los buzones de correo electrónico privado. La red local privada 105 puede ser así visualizada como un sitio de acceso protegido dentro de la Internet. Se hace notar que esto es meramente un ejemplo, el procedimiento de autenticación que va a ser descrito teniendo una aplicabilidad muy general; a este respecto, el usuario remoto USERa pudiera ser cualquier usuario autorizado de los servicios proporcionados por la red local privada 105, tal como un cliente del dueño de la red local privada 105 que desea, por ejemplo, inspeccionar una condición de pedidos de compra efectuados.

[0034] De acuerdo con una realización de la presente invención, con fines de autenticación, el usuario remoto USERa es provisto de un par de módulos de identificación de suscriptor, particularmente (aunque no limitativamente) Módulos de Identidad de Suscriptor (SIM) del tipo usado con fines de autenticación en Sistemas telefónicos Celulares Digitales (DCS por sus siglas en inglés) o Redes Móviles Terrestres Públicas (PLMN por sus siglas en inglés), tales como las redes telefónicas celulares ampliamente difundidas del Sistema Global para comunicaciones Móviles (GSM por sus siglas en inglés), o extensiones conocidas de las mismas tales como las redes de Servicio General de Radio en Paquetes (GPRS por sus siglas en inglés) (que son actualmente una sub-red de la red GSM), o las redes del Sistema Universal de Telecomunicaciones Móviles (UMTS por sus siglas en inglés) (un sistema de comunicaciones celulares de tercera generación, de banda ancha), o una red de comunicaciones móviles basada en satélite.

[0035] Tal como se sabe en el arte, un SIM adopta normalmente la forma de una tarjeta (del tamaño de una tarjeta de crédito o más pequeña, dependiendo de la escala de miniaturización del terminal de usuario), con componentes de circuitos integrados empotrados, que almacena particularmente datos personalizados que soportan la autenticación del SIM, así como codificación y decodificación. Por lo menos hasta el presente, el uso de un SIM (y del procedimiento de autenticación basado en SIM) para identificar un terminal de comunicaciones móviles acoplado al mismo ha demostrado ser una manera robusta para imposibilitar que otros dispositivos se hagan pasar por ese terminal, proporcionando así un acceso autenticado seguro a, por ejemplo, una cuenta correspondiente a ese usuario particular.

[0036] Un primer SIM SIMa del par de SIM del usuario está acoplado operativamente (de manera removible) a la computadora 140 de usuario remoto; por ejemplo, el primer SIM SIMa es empotrado en un dispositivo periférico de computadora que puede ser acoplado operativamente a la computadora 140, de modo a ser funcionalmente asequible por la misma, por ejemplo una tecla de hardware 145 que puede ser conectada a un puerto (no mostrado explícitamente en la Figura 1) de la computadora 140, por ejemplo un puerto de Colector Serial Universal (USB por sus siglas en inglés), o un puerto PCMCIA de la misma, o por medio de un periférico del tipo lector de tarjeta inteligente y adaptado para interactuar con un SIM, o el primer SIM SIMa puede ser empotrado en una tarjeta de memoria que puede ser entonces acoplada operativamente a la computadora 140 por medio de un lector de tarjeta de memoria. Se hace notar que la forma específica en que el primer SIM SIMa es acoplado operativamente a la computadora 140 no es limitativo para la presente invención, siendo en general suficiente que el primer SIM SIMa

sea acoplado operativamente a la computadora 140 (de una manera adecuada para permitir la comunicación entre la computadora 140 y el SIM SIMa) por medio de cualquier tipo de dispositivo adaptador/lector conectado a la computadora 140 a través de cualquier tipo de puerto periférico.

[0037] Un segundo SIM SIMb es insertado (de manera removible) en un terminal 150 de comunicación/teléfono móvil del usuario, tal como un teléfono móvil adaptado para ser usado en una red de comunicación móvil (por ejemplo una PLMN) 155, tal como una red de teléfono celular de GSM, una red de GPRS o una red de UMTS, operada por un operador de red de GSM (o GPRS, o UMTS).

[0038] De acuerdo con una realización de la presente invención, una relación uno a uno existe entre los SIM primero y segundo SIMa y SIMb, y entre los dos SIM SIMa y SIMb y el usuario USERa, en el sentido de que la autoridad que expide los dos SIM, normalmente pero no estrictamente necesariamente el operador de la red de GSM, no solamente considera que cada uno de los dos SIM está asociado con ese usuario suscriptor particular USERa, sino que adicionalmente los dos SIM SIMa y SIMb del par de SIM son considerados como asociados uno con el otro. Se hace notar que, aunque en el ejemplo de realización de la invención discutido en la presente se considera un operador 160 de red de GSM único, esto no debe ser considerado como una limitación de la presente invención; diferentes operadores de red de GSM (o GPRS, o UMTS) pueden cooperar para proporcionar el servicio de autenticación segura de usuario, a condición de que la asociación antes citada entre los dos SIM, y entre el par de SIM y el usuario, sea garantizada.

[0039] De manera más general, es suficiente que se mantenga una relación (en algún tipo de base de datos, manejada por ejemplo por el operador de la red de GSM) entre los datos del primer SIM SIMa y una identificación (típicamente, el número de teléfono) que permite contactar un terminal de comunicación móvil del usuario que está acoplado al segundo SIM SIMb.

[0040] También se muestra en el dibujo una computadora de servidor de autenticación 165 (de manera más general, un sistema de procesamiento de datos de autenticación, que comprende por ejemplo una red de computadoras) que maneja (por lo menos parcialmente) un procedimiento de autenticación de usuario en dos pasos basado en los dos SIM SIMa y SIMb, dicho procedimiento siendo descrito en detalle más adelante. En términos extremadamente generales, la computadora de servidor de autenticación 165 está conectada a la Internet 135 y, en el ejemplo mostrado, es parte del operador de red de GSM 160 (en cuyo caso el servicio de autenticación es uno de los servicios proporcionados por el operador de red de GSM), aunque en general la computadora de servidor de autenticación 165 no es necesariamente parte del operador de red de GSM 160, sino que meramente se comunica con el mismo (por un enlace de comunicación segura, tal como, por ejemplo, una Red Privada Virtual).

[0041] La Figura 2 ilustra esquemáticamente, en términos de los bloques funcionales pertinentes para el entendimiento del procedimiento de autenticación de acuerdo con la realización de la invención descrita en la presente, el operador de red de GSM 160 y la computadora de servidor de autenticación 165.

[0042] La computadora de servidor de autenticación 165 está adaptada para llevar a cabo una autenticación basada en SIM de la computadora remota 140. Tal como se discutió en la parte introductoria de la presente descripción, el mecanismo de autenticación basado en SIM de un terminal de procesamiento de datos de usuario, tal como la computadora remota 140, es conocido per se, y un ejemplo de una estructura que permite implementar tal mecanismo es proporcionado en la solicitud internacional ya citada WO 00/02406. Sin entrar en detalles específicos, la computadora de servidor de autenticación 165 comprende un servidor de autenticación 200 que está conectado tanto a la Internet 135 como (a través de una conexión segura 203) a un servidor delegado 210, que tiene acceso a un centro de autenticación 215 del operador de red de GSM 160, dicho centro de autenticación 215 estando a su vez conectado a un Registro de Localización de Origen (HLR por sus siglas en inglés) del operador de red de GSM 160. La conexión segura 205 es por ejemplo asegurada por el hecho de que el servidor de autenticación 200 es colocado físicamente próximo al servidor delegado 210. El centro de autenticación 215 es el centro de autenticación de la red de GSM normalmente utilizado de manera confiable para llevar a cabo procedimientos estándar de autenticación de los terminales de comunicaciones móviles equipados con SIM de los usuarios (teléfonos móviles), tales como el teléfono móvil 150, que desean ser conectados a la red de GSM 155. El servidor delegado 210 permite una conexión entre el servidor de autenticación 200 y la red de GSM, y en particular encamina el tráfico entre el servidor de autenticación 200 y el centro de autenticación de GSM 215; el servidor delegado 210 actúa como un Registro de Localización de Visitante (VLR por sus siglas en inglés) virtual, luciendo para el HLR del operador de la red de GSM como cualquier otro VLR de la red de GSM. Las comunicaciones 220 entre el servidor delegado 210 y el centro de autenticación 215 de GSM pueden tener lugar por la red de señalización SS7 normalizada utilizada por el operador de red de GSM. Una base de datos 225 está asociada con el servidor de autenticación 200, usada para almacenar datos de autenticación de usuario durante el procedimiento de autenticación.

[0043] La computadora de servidor de autenticación 165 también incluye un servidor asociador de SIM 230, el cual, en conexión con una base de datos de pares de SIM 235 que almacena información sobre los pares de SIM tales

como el par de SIM SIMa y SIMb (o, más simplemente, la identificación, por ejemplo el número de teléfono móvil correspondiente al segundo SIM SIMb que está asociado con el primer SIM SIMa), es capaz de identificar un SIM de un par de SIM dado, por ejemplo el segundo SIM SIMb (o el número de teléfono móvil correspondiente al mismo), en base a información que identifica al otro SIM, en este ejemplo el primer SIM SIMa, proporcionada por el servidor de autenticación 200. El servidor asociador de SIM 230 se comunica con un agente generador de claves 235, que genera unas claves (preferentemente, que pueden ser usadas sólo una vez) a ser enviadas por la red de GSM 155 al teléfono móvil 150 del usuario, por ejemplo en forma de un mensaje del Servicio de Mensajes Cortos (SMS), preparado por un agente compilador de SMS 245. El mensaje es entregado al receptor propuesto por un centro de servicio de mensajería 250 del operador 160 de red de GSM, por ejemplo un centro de SMS, o un centro de Servicio de Mensajería de Multimedia (MMS por sus siglas en inglés), para distribuir mensajes de texto o de multimedia a los terminales de suscriptores de la red de GSM 155. Alternativamente, las claves pueden ser enviadas en forma de MMS, o pueden ser comunicadas al usuario a través de llamadas telefónicas, por ejemplo operando un sintetizador de voz. Se proporciona un agente comparador de claves 255 para comparar las claves generadas por el agente generador de claves 240 con las claves de respuesta correspondientes, introducidas por el usuario y recibidas por la Internet 235, por ejemplo por medio del servidor de autenticación 200.

[0044] Se hace notar que por lo menos algunos de los bloques funcionales de la computadora de servidor de autenticación 165 descritos anteriormente pueden ser, y normalmente serían, implementados como una mezcla de hardware y software, o incluso totalmente como software.

[0045] La Figura 3 es una vista gráfica esquemática simplificada del contenido de una memoria de trabajo 300 (por ejemplo, una RAM) de la computadora remota 140 durante el proceso de autenticación. Un módulo 305 de software de Interfaz Gráfica de Usuario (GUI por sus siglas en inglés) permite una fácil interacción del usuario USERa con la computadora 140, a través de periféricos de computadora de entrada/salida convencionales, esquematizados como un bloque 310 y que incluyen un monitor, un teclado, un dispositivo apuntador. Un módulo 315 de software de unidad USB permite la interacción con los periféricos USB, en este ejemplo la tecla USB 145 que tiene el primer SIM SIMa empotrado en la misma. Un módulo 320 de software de unidad de módem perite la comunicación con un módem 325 (por ejemplo ISDN o XDSL), usado para la conexión al punto de acceso 130b; el módulo de unidad de módem maneja los detalles de bajo nivel de la comunicación. Un módulo 330 de software de comunicación con Internet maneja en cambio los detalles de nivel superior de la comunicación por la Internet, por ejemplo los detalles relacionados con el Protocolo de Internet (IP por sus siglas en inglés). El bloque 335 esquematiza una aplicación de software que está operando en la computadora 149 y que se supone que ha solicitado servicios a un sitio protegido que proporciona acceso selectivo a los servicios, condicionado a una autenticación preliminar del usuario; por ejemplo, la aplicación 335 es un software de cliente de correo electrónico (por ejemplo Outlook o Outlook Express por Microsoft, Eudora, LotusNotes) que el usuario USERa de la computadora 140 ha iniciado para tener acceso al buzón de correo electrónico personal mantenido por el servidor de correo 110. El bloque 340 esquematiza en cambio una aplicación de software de cliente de autenticación que es invocada en la computadora 140, por ejemplo en respuesta a una solicitud de autenticación del servidor de correo 110, de modo a manejar esa parte del procedimiento de autenticación local a la computadora 140, como se describe en detalle más adelante. Esquemáticamente, el cliente de autenticación 340 comprende un agente de dialogado con SIM 345, para dialogar con el SIM SIMa en la tecla USB 145, y un módulo 350 de búsqueda y encaminado de clave, para buscar, por ejemplo, una clave introducida por el usuario, por ejemplo a través del teclado, y encaminar la clave introducida al módulo de comunicación 330, de modo a hacer que la clave sea enviada a la computadora de servidor de autenticación 165 por la Internet 135.

[0046] Se observa que todos los módulos de software son instalados preliminarmente en la computadora 140, y, cuando son invocados, operan sobre la parte superior de un sistema operativo de computadora, no esquematizado explícitamente en el dibujo. En particular, el software 340 de cliente de autenticación, que puede ser instalado desde un soporte físico, tal como un disco flexible, un CD-ROM o DVD-ROM, o descargándolo desde un servidor de archivo adecuado (por ejemplo, por medio de una sesión FTP), en algunos casos puede adoptar la forma de un dispositivo de inserción para una aplicación de solicitud de servicio 335 ya existente, por ejemplo un dispositivo de inserción para un cliente de correo tal como Microsoft Outlook, Microsoft Outlook Express, Eudora, Lotus Notes, o para un navegador tal como Microsoft Internet Explorer o Netscape Communicator.

[0047] A continuación, un ejemplo de procedimiento de autenticación de acuerdo con una realización de la presente invención será descrito con la ayuda de los diagramas de flujo de la Figura 4, considerando el escenario esbozado hasta ahora.

[0048] Asúmase que el usuario USERa, en una localización remota de la red local privada 105 del patrono, desea conectarse con el servidor de correo 110 para revisar su buzón electrónico personal. El usuario USERa establece una conexión a la Internet 135 (a través del punto de acceso 130b), entonces inicia el cliente de correo electrónico 335, el cual trata de obtener acceso al servidor de correo 110 en la red local privada 105 (el sitio protegido, bloque 401 en la Figura 4). El servidor de correo 110 recibe la solicitud de acceso (bloque 403) y, antes de conceder

acceso a (el cliente de correo electrónico 335 que opera en) la computadora remota 140, comienza el procedimiento de autenticación emitiendo una solicitud de autenticación a la computadora 140. Entonces, el servidor de correo 110 espera una confirmación de autenticación (bloque 405), a ser recibida desde la computadora de servidor de autenticación 165.

[0049] El procedimiento de autenticación está compuesto por dos fases de autenticación: una primera fase de autenticación proporciona una autenticación basada en SIM de la computadora 140, llevada a cabo basándose en el procedimiento de autenticación operado en la red de GSM 155 para autenticar teléfonos móviles de usuarios. Una vez que la computadora 140 ha sido autenticada, una segunda fase de autenticación proporciona la autenticación (identificación o reconocimiento personal) del usuario USERa de la computadora 140.

[0050] Con el fin de comprender los detalles del procedimiento de autenticación basado en SIM de la computadora 140, es útil revisar brevemente la forma en que los teléfonos móviles son normalmente autenticados en una red de GSM.

[0051] Cuando un teléfono móvil de un usuario, por ejemplo el teléfono móvil 150 del usuario USERa, trata de conectarse con una red de GSM, tal como la red de GSM 155, el centro de autenticación 215 del operador 160 de red de GSM le pide al teléfono móvil 150 que proporcione la Identidad de Suscriptor Móvil Internacional (IMSI por sus siglas en inglés) respectiva, la cual es un código identificador de nueve bits almacenado en el SIM del teléfono móvil SIMb. En respuesta, el teléfono móvil 150 proporciona al operador 160 de la red de GSM el código identificador IMSI solicitado. El centro de autenticación 215 usa el código IMSI recibido para generar el llamado triplete de autenticación, compuesto por un "desafío", una "respuesta firmada" y una clave de codificación; el desafío es un valor aleatorio de dieciséis bits, la clave de codificación es la clave de codificación específica de la conexión usada en la red de GSM 155, y la respuesta firmada (en adelante, simplemente respuesta) es un valor de cuatro bytes que es derivado del desafío usando la clave de codificación específica. El centro de autenticación 215 envía entonces el desafío al teléfono móvil 150; en base al desafío recibido desde el centro de autenticación 215, el SIM del teléfono SIMb genera una respuesta y una clave de codificación: la clave es almacenada en el SIM SIMb, mientras que la respuesta es transmitida de regreso al centro de autenticación 215. El centro de autenticación 215 compara la respuesta recibida con una respuesta generada localmente (la respuesta firmada generada en el proceso de generación de triplete), y si las dos respuestas coinciden, la autenticación del SIM SIMb es completada con éxito.

[0052] Regresando a la Figura 4, la computadora remota 140 recibe la solicitud de autenticación desde el servidor de correo 110 (bloque 409); esto causa que el cliente de autenticación 340 sea invocado, por ejemplo por medio de una instrucción incluida en una página Web descargada a la computadora remota 140 cuando esta última se pone en contacto con el servidor de correo 110, y que la conexión de la computadora remota 140 al servidor de correo 110 sea redirigida al servidor de autenticación 200 en la computadora de servidor de autenticación 165; la computadora remota 140 se pone así en contacto con el servidor de autenticación 200 y le proporciona la dirección de IP de la misma, pidiendo al servidor de autenticación 200 que autentique de manera segura al usuario USERa (y proporcione confirmación de la autenticación al servidor de correo 110) (bloque 411). El servidor de autenticación 200 recibe la solicitud de autenticación desde la computadora 140, junto con la dirección de IP de la misma, la cual será usada para identificar la computadora 140 al servidor de correo 110 (bloque 413).

[0053] La autenticación basada en SIM de la computadora 140 (primera fase del procedimiento de autenticación) es similar a la autenticación explicada previamente del teléfono móvil 150 para la conexión a la red de GSM 155, excepto que en este caso los datos viajan parcialmente por la Internet 135 (de manera más general, una red de computación abierta), y no solamente por la red de GSM 155.

[0054] El servidor de autenticación 200 expide (bloque 415) a la computadora 140 una solicitud para datos de identificación del primer SIM SIMa del par de SIM de autenticación, a saber, el SIM acoplado operativamente a la computadora 140. El cliente de autenticación 340 recibe la solicitud y entonces obtiene acceso al primer SIM SIMa empotrado en la tecla USB 145 para leer desde el mismo los datos de identificación, tales como la IMSI (bloque 417). Si el cliente de autenticación 340 no puede encontrar un SIM vinculado a la computadora 140, un mensaje puede ser generado al usuario USERa pidiendo la conexión del periférico que porta el SIM a la computadora 140, o la inserción del primer SIM SIMa en un lector adecuado. El cliente de autenticación 340 envía entonces los datos de identificación leídos desde el primer SIM SIMa al servidor de autenticación 200 (bloque 419).

[0055] Con el fin de autenticar el primer SIM SIMa, el servidor de autenticación 200 presenta los datos de identificación del primer SIM recibidos desde la computadora 140 al centro de autenticación de GSM 215 en las premisas del operador de GSM 150 (bloque 421). Con este fin, el VLR virtual 210 es aprovechado para establecer una conexión entre el servidor de autenticación 200 y el centro de autenticación de GSM 215. El servidor de autenticación 200 envía al VLR virtual 210 un mensaje de solicitud de autenticación, que contiene los datos de identificación (la IMSI) del primer SIM SIMa a ser autenticado, tales como fueron recibidos desde la computadora 140. El VLR virtual 210 envía al centro de autenticación de GSM 215 un mensaje de indagación adecuadamente

formateado (por ejemplo, un mensaje de acuerdo con el protocolo de la Parte de Aplicación de Móvil (MAP por sus siglas en inglés)), para solicitar al centro de autenticación de GSM 215 que emita un triplete de autenticación. El centro de autenticación de GSM 215 recibe el mensaje de indagación que contiene la IMSI del primer SIM SIMa, y responde generando (bloque 423) y enviando (bloque 425) al VLR virtual 210 en la computadora de servidor de autenticación 165 un triplete de autenticación, totalmente similar a aquéllos usados para registrar teléfonos móviles a la red de GSM 155, y compuesto por un desafío, una respuesta y una clave de codificación. El triplete de autenticación es enviado por el VLR virtual 210 al servidor de autenticación 200, el cual almacena el triplete de autenticación (bloque 427) y, desde ese momento, actúa con respecto al primer SIM SIMa de la misma manera en que el centro de autenticación de GSM 215 actuaría con respecto a un teléfono móvil a ser autenticado. El desafío es enviado por la Internet 135 a la computadora 140 (bloque 427), en la cual el cliente de autenticación 340 encamina el desafío recibido al primer SIM SIMa (bloque 429).

[0056] Cuando el primer SIM SIMa recibe el desafío, genera una clave de codificación y una respuesta (bloque 431); la clave de codificación es almacenada en el primer SIM SIMa o en el cliente de autenticación 340 (por ejemplo para ser usada para codificar futuras comunicaciones por la Internet con el sitio protegido), y la respuesta generada es enviada de regreso por el cliente de autenticación 340 al servidor de autenticación 200 (bloque 433).

[0057] Cuando el servidor de autenticación 200 recibe desde el cliente de autenticación 340 la respuesta generada por el primer SIM SIMa (bloque 435), la respuesta recibida es comparada con la respuesta construida en el triplete de autenticación (bloque 437). Si las dos respuestas no coinciden (ramal de salida N del bloque de decisión 439), el servidor de autenticación 200 informa al sitio protegido 110 (aprovechando la dirección de IP de la computadora remota 140) que la autenticación de primer nivel falló (bloque 441); si el servidor de red privada 110 recibe tal mensaje (bloque 443, ramal de salida S), niega el acceso de la computadora de usuario 140 (identificada por la dirección de IP respectiva) a los servicios (bloque 445). Si, en cambio, las dos respuestas coinciden (ramal de salida S del bloque de decisión 439), el servidor asociador de SIM 230 en la computadora de servidor de autenticación 165 recupera de la base de datos 235 de pares de SIM la información de identificación del segundo SIM SIMb del usuario (bloque 447); por ejemplo, el número de teléfono móvil correspondiente al segundo SIM SIMb es identificado, de modo a permitir la puesta en contacto con el usuario por el teléfono móvil 150 del usuario. El agente generador de clave 240 genera entonces la clave a ser enviada al usuario remoto USERa a través del teléfono móvil personal 150 (bloque 449). El compilador de mensajes de SMS 245 compila entonces un mensaje de SMS a ser enviado al teléfono móvil 150 del usuario USERa, que contiene la clave generada, y envía el mensaje al teléfono móvil 150 del usuario (bloque 451); el centro de SMS 240 del operador de GSM 160 entrega el mensaje de SMS al teléfono móvil 150 del usuario (bloque 453).

[0058] En paralelo, el cliente de autenticación 340 hace que un mensaje de invitación sea mostrado al usuario USERa de la computadora 140 para invitarle a introducir la clave recibida por el teléfono móvil personal 150 (bloque 455). Condicionado al hecho de que el teléfono móvil 150 del usuario haya sido registrado preliminarmente en la red de GSM (en la forma convencional indicada en lo precedente), el mensaje de SMS proveniente de la computadora de servidor de autenticación 165 con la clave a ser usada para completar el procedimiento de autenticación es recibido en el teléfono móvil 150 del usuario. En una realización de la presente invención, el mensaje de SMS está codificado, para mayor seguridad.

[0059] Cuando el usuario USERa recibe la clave, introduce la clave en la computadora 140, y el cliente de autenticación 340 acepta la clave introducida y la envía al servidor de autenticación 200, por la Internet (bloque 457). Se hace notar que no es estrictamente necesario que la clave introducida por el usuario coincida con la clave recibida en el teléfono móvil: el usuario puede ser provisto, de hecho, de un dispositivo de encriptado (por ejemplo, una tabla de transcódigo), mediante el cual, para cualquier clave recibida, una clave encriptada puede ser derivada.

[0060] La clave es recibida en el servidor de autenticación 200 (bloque 459), y es comparada por el agente comparador de claves 255 con la clave originada localmente (bloque 461). Si las dos claves no coinciden (ramal de salida N del bloque de decisión 463), el servidor de autenticación 200 informa al servidor 110 del sitio protegido que la autenticación de segundo nivel falló (bloque 465); si el servidor de red privada 110 recibe tal mensaje (bloque 467, ramal de salida S), niega el acceso de la computadora de usuario 140 a los servicios (bloque 469). Si, en cambio, las dos respuestas coinciden (ramal de salida S del bloque de decisión 463), la autenticación del usuario USERa es exitosa, y el servidor de autenticación 200 informa al servidor 110 del sitio protegido que el usuario USERa, identificado de manera única con esa dirección de IP específica, ha sido autenticado con éxito (bloque 471). Con el fin de prevenir cualquier fraude, esta confirmación de autenticación del servidor de autenticación 200 al sitio protegido 110 puede ser comunicada a través de una conexión segura 170 (representada con puntos y rayas), o ser encriptada; por ejemplo, una Red Privada Virtual (VPN por sus siglas en inglés) puede ser establecida entre el servidor del sitio protegido que solicita la autenticación y el servidor de autenticación.

[0061] Cuando el servidor 110 del sitio protegido recibe tal confirmación, concede acceso a los servicios (bloque 473), permitiendo por ejemplo que el cliente de correo electrónico 335 tenga acceso al buzón personal del usuario

USERa. A partir de ese momento, el usuario autenticado USERa puede aprovechar los servicios ofrecidos por el servidor 110.

[0062] Se hace notar que, en vez de aprovechar la dirección de IP de la computadora remota 140 como una forma para identificar la computadora en el sitio protegido y el servidor de autenticación (una solución que, en algunos casos, puede plantear algunos problemas, tal como en el caso de que la computadora 140 se conecte a la Internet pasando a través de un servidor delegado, o, en general, cada vez que la conexión es efectuada a través de un dispositivo que filtra las direcciones de IP), unas soluciones diferentes pueden ser adoptadas, basándose por ejemplo en un intercambio de datos de identificación a un nivel superior con respecto al nivel de IP, por ejemplo un nivel de aplicación.

[0063] Se puede apreciar que el procedimiento de autenticación descrito anteriormente se basa en un proceso de autenticación en dos pasos: un primer procedimiento de autenticación basado en SIM para autenticar la computadora remota 140, y un segundo procedimiento de autenticación, que aún se basa en una autenticación de SIM (la autenticación del teléfono móvil del usuario para la conexión a la red de GSM), mediante el cual la identidad del usuario es asegurada (con el fin de tener un acceso concedido, un usuario fraudulento no solamente debería estar en posesión del primer SIM SIMa, sino también del segundo SIM SIMb, considerándose que dicha ocurrencia es muy poco probable). También, la clave (que preferentemente puede ser usada sólo una vez) necesaria para completar la autenticación es comunicada al usuario por un enlace autenticado y seguro tal como la red de GSM; para una seguridad aún mayor, se puede proporcionar un encriptado de la clave. Adicionalmente, un código de Número de Identificación Personal (PIN por sus siglas en inglés) podría ser solicitado al usuario, con el fin de obtener acceso al primer SIM SIMa asociado con la computadora 140, para mejorar aún más la seguridad.

[0064] Tal como ya se mencionó, el centro de autenticación de GSM usado para autenticar el primer SIM SIMa no necesita ser necesariamente el mismo centro de autenticación de GSM que autentica el segundo SIM SIMb, a condición de que la relación entre los dos SIM sea garantizada.

[0065] Con el fin de aumentar la seguridad de las transacciones, los datos intercambiados entre la computadora 140 y el servidor 110 del sitio protegido, una vez que la autenticación ha sido completada y el acceso a los servicios deseados es concedido, pueden ser encriptados, por ejemplo usando la misma clave de encriptado generada por el primer SIM SIMa.

[0066] El Solicitante indica que el procedimiento de autenticación segura en dos pasos de acuerdo con la presente invención tiene una aplicabilidad muy amplia, no estando limitado al ejemplo de escenario considerado en la presente. Por ejemplo, el procedimiento puede ser aprovechado no solamente para autenticar a un usuario remoto que tiene acceso a la red local privada 105 a través de la Internet, sino incluso a través de una conexión de marcado directo a la red local privada.

[0067] El procedimiento de autenticación segura de acuerdo con la presente invención puede ser aprovechado incluso en caso de que el acceso a la red local privada no ocurra a través de una red abierta insegura tal como la Internet, sino que la computadora del usuario esté dentro de la red 105 y conectada directamente a la misma, para hacer segura una conexión normal del usuario: en este caso, la red externa puede ser involucrada meramente con el fin de comunicarse con la computadora de servidor de autenticación 165. Esta situación es esquemáticamente ilustrada en la Figura 1, en la cual la referencia USERb denota un usuario local de la red local privada 105, por ejemplo un empleado del dueño de la empresa de la red local privada 105, que desea conectarse a la red a través de una de las computadoras de la misma, por ejemplo la computadora de cliente 110a, de modo a aprovechar los servicios puestos a la disposición por el sistema de procesamiento de datos de la empresa (entre dichos servicios, la conectividad a la Internet 135 pudiendo estar incluida). Al igual que el usuario remoto USERa, también el usuario USERb es provisto de un par de SIM: un primer SIM (empotrado por ejemplo en una tecla de USB adaptada para ser leída por la computadora 110a) para la autenticación basada en SIM de la computadora que abre la sesión, y un segundo SIM a ser usado en un teléfono móvil de usuario convencional, para recibir, por la red del teléfono móvil, la clave desde la computadora de servidor de autenticación 165.

[0068] También se observa que, aunque en el escenario considerado en la presente la computadora de servidor de autenticación estaba afuera del ambiente de procesamiento de datos que solicitaba autenticación, y particularmente era parte del operador de red de GSM, esto no es considerado como limitativo para la presente invención; de hecho, la computadora o sistema de computadoras de servidor de autenticación puede ser parte del sistema de procesamiento de datos de, por ejemplo, la empresa que implementa el procedimiento de autenticación segura de la presente invención.

[0069] El procedimiento de autenticación de acuerdo con la presente invención está particularmente adaptado para asegurar un alto grado de seguridad en las transacciones llevadas a cabo por empleados de una empresa o una agencia gubernamental. Así, el procedimiento de autenticación de acuerdo con la presente invención proporciona una forma adecuada para manejar la seguridad de una empresa o agencia en conexión con el personal de la misma.

[0070] Sin embargo, esta aplicación del procedimiento de autenticación no es limitativa; por ejemplo el procedimiento puede ser usado para autenticar clientes de sitios de Internet de comercio electrónico.

[0071] También se indica que, aunque en el ejemplo de realización descrito en lo precedente la clave (para ser usada una sola vez) es recibida por el usuario en el teléfono móvil personal, y el usuario tiene que introducir la clave personalmente en la computadora 140, esto no debe ser considerado como una limitación de la presente invención; nada impide de hecho la provisión de que la clave recibida a través de la red de GSM sea introducida automáticamente a la computadora, por ejemplo conectando operativamente el teléfono móvil 150 del usuario a la computadora 140 del usuario, por ejemplo mediante una conexión Bluetooth o similar.

[0072] En conclusión, la presente invención ha sido descrita en la presente por medio de algunas realizaciones, y algunas alternativas han sido expuestas, pero es evidente para aquéllos versados en el arte que diversas modificaciones a las realizaciones descritas, así como otras realizaciones de la presente invención, son posibles sin apartarse del alcance de la misma como se define en las reivindicaciones anexas.

REIVINDICACIONES

1. Procedimiento mediante el cual un terminal de procesamiento de datos (**140**) de un usuario (USERA;USERb) en un sistema de procesamiento de datos es autenticado con la finalidad de darle acceso a servicios seleccionados proporcionados por el sistema de procesamiento de datos (**100**, **105**), comprendiendo el procedimiento:

interactuar (**417**, **419**, **929**, **431**, **433**) con un primer módulo de identidad de suscriptor de usuario (**SIMa**) operativamente asociado con el terminal de procesamiento de datos, y con un servidor de procesamiento de datos de autenticación en el sistema de procesamiento de datos, para realizar una primera autenticación basada en SIM del terminal de procesamiento de datos de usuario;

adquirir (**455**) una primera información de identidad personal proporcionada al usuario en un terminal de comunicación móvil de usuario (**150**) autenticado a través de una red de comunicación móvil (**155**) empleando un segundo Módulo de identidad de suscriptor (**SIMb**) suministrado al usuario, mediante el cual el primer módulo de identidad de suscriptor es asociado con información de identificación del segundo Módulo de Identidad de Suscriptor, siendo dicha primera información de identidad personal proporcionada al usuario aprovechando la asociación entre el primer módulo de identidad de suscriptor y el segundo Módulo de identidad de suscriptor y extraer dicha información de identificación del segundo Módulo de identidad de suscriptor para permitir entrar en contacto con el usuario por el terminal de comunicación móvil, y en respuesta a dicha adquisición de la primera información de identificación personal, enviar (**457**) segunda información de identificación personal al servidor de procesamiento de datos de autenticación para completar la autenticación del terminal de procesamiento de datos y concederle el acceso a los servicios seleccionados.

2. El procedimiento según la reivindicación 1, que comprende además:

extraer (**417**) Datos de identificación SIM del primer módulo de identidad de suscriptor (**SIMa**);

comunicar (**419**) los datos de identificación SIM extraídos al servidor de autenticación, el servidor de autenticación actuando como un centro de autenticación (**215**) de una red de operador de comunicación móvil (**160**);

recibir (**429**) del servidor de autenticación datos de autenticación SIM correspondientes a los datos de identificación SIM , y pasar (**431**) los datos de autenticación SIM al primer Módulo de Identidad de Suscriptor; y

comunicar (**433**) al servidor de autenticación una respuesta generada por el primer Módulo de Identidad de Suscriptor.

3. Un procedimiento mediante el cual un servidor de procesamiento de datos de autenticación (**165**) autentica un terminal de procesamiento de datos de usuario (**140**) de un usuario (USERA;USERb) en un sistema de procesamiento de datos (**100**) con la finalidad de conceder al terminal de procesamiento de datos acceso a servicios seleccionados proporcionados por el sistema de procesamiento de datos (**100**, **105**), comprendiendo el procedimiento:

recibir (**413**) una solicitud de autenticación del terminal de procesamiento de datos, teniendo el terminal de procesamiento de datos operativamente asociado un primer módulo de identidad de suscriptor (**SIMa**);

realizar una primera autenticación basada en SIM del terminal de procesamiento de datos basada en los datos asociados con el primer Módulo de Identidad de Suscriptor;

proporcionar (**447**, **449**, **451**) al usuario una primera información de identidad personal aprovechando un terminal de comunicación móvil de usuario (**150**) autenticado en una red de comunicación móvil (**155**) empleando un segundo Módulo de identidad de suscriptor (**SIMb**) suministrado al usuario, mediante el cual el primer módulo de identidad de suscriptor es asociado con información de identificación del segundo Módulo de Identidad de Suscriptor, y en el que dicha información de identificación personal es proporcionada al usuario aprovechando la asociación entre el primer módulo de identidad de suscriptor y el segundo Módulo de identidad de suscriptor y extraer dicha información de identificación del segundo Módulo de identidad de suscriptor para permitir entrar en contacto con el usuario por el terminal de comunicación móvil, y condicionar (**459**, **461**, **463**) la autenticación del terminal de procesamiento de datos de usuario para conceder a este el acceso a los servicios seleccionados a la primera autenticación basada en SIM y a una segunda autenticación basada en una correspondencia prescrita entre la primera información de identidad personal proporcionada al usuario y segunda información de identificación personal recibida del terminal de procesamiento de datos de usuario en respuesta a la provisión de la primera información de identificación personal.

4. El procedimiento según la reivindicación 3, en el que el servidor de procesamiento de datos de autenticación acting (**415**, **421**, **427**, **435**, **437**, **439**) as un centro de autenticación (**215**) de una red de operador de comunicación móvil (**160**).

5. El procedimiento según la reivindicación 4, en el que el: dicha provisión al usuario de una primera información de identidad personal comprende generar en el servidor de procesamiento de datos de autenticación una primera palabra clave y enviar la primera palabra clave sobre la red de comunicación móvil al terminal de comunicación móvil del usuario; dicha segunda información de identificación personal es una segunda palabra clave, dependiendo de la primera palabra clave, entrada en el terminal de procesamiento de datos y proporcionados al servidor de procesamiento de datos de autenticación a través del sistema de procesamiento de datos, y dicho condicionamiento dela autenticación del terminal de procesamiento de datos en el sistema de procesamiento de datos comprende condicionar la autenticación a una correspondencia prescrita entre la primera palabra clave y la segunda palabra clave.

6. Procedimiento de autenticación de un terminal de procesamiento de datos (**140**; **115a**) de un usuario (**USERa**; **USERb**) para conceder al terminal de procesamiento de datos acceso a servicios seleccionados proporcionados por un sistema de procesamiento de datos (**100**, **105**), estando provisto el usuario de un terminal de comunicación móvil autenticable (150) adaptado para ser utilizado en una red de comunicación móvil (155), comprendiendo el procedimiento:

hacer que el terminal de procesamiento de datos realice las acciones del procedimiento según la reivindicación 1; y

hacer que el servidor de procesamiento de datos (**165**) del sistema de procesamiento de datos realice las acciones del procedimiento según la reivindicación 3.

7. El procedimiento según la reivindicación 6, en el que dicha segunda autenticación comprende:

proporcionar al usuario la primera información de identidad personal mediante:

generación (**449**) de una primera palabra clave en el servidor de procesamiento de datos de autenticación y

enviar (**451**, **453**) la primera palabra clave al terminal de comunicación móvil sobre la red de comunicación móvil; y

verificar (**459**, **461**) una correspondencia entre la primera palabra clave y dicha segunda información de identificación personal, en el que la segunda información de identificación personal es una segunda palabra clave, dependiendo de la primera palabra clave, entrada (**457**) en el terminal de procesamiento de datos y proporcionada al servidor de procesamiento de datos de autenticación a través del sistema de procesamiento de datos.

8. El procedimiento según la reivindicación 7, que comprende que el usuario entre la segunda palabra clave a través del terminal de procesamiento de datos.

9. El procedimiento según la reivindicación 7, en el que la segunda palabra clave es entrada automáticamente tras recibir la primera palabra clave en el terminal de comunicación móvil del usuario.

10. El procedimiento según la reivindicación 7, 8 o 9, en el que dicha primera palabra clave es utilizable una cantidad de veces limitada, particularmente solo una vez.

11. El procedimiento según cualquiera de las reivindicaciones anteriores 6 a 10, en el que el segundo Módulo de identidad de suscriptor tiene una relación uno a uno fijada con el primer Módulo de Identidad de Suscriptor.

12. El procedimiento según cualquiera de las reivindicaciones anteriores 6 a 11, en el que dicha información de identificación del segundo Módulo de identidad de suscriptor es un número de terminal de comunicación móvil.

13. El procedimiento según cualquiera de las reivindicaciones anteriores 6 a 12, en el que dicha primera información de identidad personal es enviada al terminal de comunicación móvil de usuario mediante mensaje de Servicio de Mensaje Corto (SMS).

14. El procedimiento según la reivindicación 13, en el que dicha realización de la primera autenticación basada en SIM del terminal de procesamiento de datos comprende tener el primer módulo de identidad de suscriptor autenticado por un servidor de autenticación (**200**) del sistema de procesamiento de datos, el servidor de autenticación actuando como un centro de autenticación (**215**) de una red de operador de comunicación móvil (**160**).

15. Sistema para autenticar un terminal de procesamiento de datos (**140**; **115a**) de un usuario (**USERa**; **USERb**) para conceder al terminal de procesamiento de datos acceso a servicios seleccionados proporcionados por el sistema de procesamiento de datos (**105**), teniendo el usuario un terminal de comunicación móvil autenticable (**150**) adaptado para ser utilizado en una red de comunicación móvil (**155**), comprendiendo el sistema:

un servidor de procesamiento de datos de autenticación (**165**) adaptado (**200**, **210**, **215**) para llevar a cabo una primera etapa de autenticación basada en un primer módulo de identidad de suscriptor (**SIMa**) operativamente asociado (**145**) con el terminal de procesamiento de datos; estando el servidor de procesamiento de datos de autenticación también adaptado (**230-245**) para:

- llevar a cabo un segundo proceso de autenticación basado en información de identificación personal proporcionada al usuario en el terminal de comunicación móvil a través de la red de comunicación móvil empleando un segundo Módulo de identidad de suscriptor (**SIMb**), en el que el primer módulo de identidad de suscriptor es asociado con información de identificación del segundo Módulo de Identidad de Suscriptor, dicha información de identificación personal siendo proporcionada al usuario utilizando la asociación entre el primer módulo de identidad de suscriptor y el segundo Módulo de identidad de suscriptor by extraer dicha información de identificación del segundo Módulo de identidad de suscriptor para permitir entrar en contacto con el usuario por el terminal de comunicación móvil, y

- conceder al terminal de procesamiento de datos acceso a los servicios seleccionados siempre que los procesos de la primera etapa de autenticación y la segunda autenticación tengan éxito.

16. El sistema según la reivindicación 15, que comprende emplear un segundo Módulo de identidad de suscriptor (**SIMb**), en el terminal de comunicación móvil para autenticar el terminal de comunicación móvil en una red de comunicación móvil (**155**).

17. El sistema según la reivindicación 16, en el que el segundo Módulo de identidad de suscriptor tiene una relación uno a uno fijada con el primer Módulo de Identidad de Suscriptor.

18. El sistema según la reivindicación 17, en el que dicha información de identificación del segundo Módulo de identidad de suscriptor es un número de terminal de comunicación móvil.

19. El sistema según cualquiera de las reivindicaciones 15 a 18, en el que dicho primer módulo de identidad de suscriptor está asociado con un dispositivo (145) conectable a la computadora a través de un puerto de conexión periférica de computadora.

20. El sistema según cualquiera de las reivindicaciones 15 a 19, en el que dicha red de comunicación móvil se selecciona de entre una red de GSM, GPRS, o UMTS.

21. Kit de autenticación para autenticar un terminal de procesamiento de datos de usuario (**140**, **115a**) en un sistema de procesamiento de datos (**100**) con la finalidad de conceder al terminal de procesamiento de datos acceso a servicios seleccionados proporcionados por el sistema de procesamiento de datos (**100**, **105**), comprendiendo el kit:

un primer módulo de identidad de suscriptor (**SIMa**);

un dispositivo de computadora periférico (**145**) que tiene asociado el primer módulo de identidad de suscriptor y asociable operativamente con el terminal de procesamiento de datos de usuario;

un segundo Módulo de identidad de suscriptor (**SIMb**) asociable operativamente con un terminal de comunicación móvil de usuario (**150**) para permitir la comunicación de este con una red de comunicación móvil (**155**), estando el primer módulo de identidad de suscriptor (**SIMa**) asociado con información de identificación del segundo Módulo de Identidad de Suscriptor, y un programa de computadora cargable directamente en una memoria de trabajo del terminal de procesamiento de datos para realizar, al ejecutarlo, un procedimiento que comprende:

interactuar con el primer módulo de identidad de suscriptor y con un servidor de procesamiento de datos de autenticación en el sistema de procesamiento de datos, para realizar una autenticación basada en SIM del terminal de procesamiento de datos de usuario;

adquirir una primera información de identidad personal proporcionada al usuario en el terminal de comunicación móvil de usuario autenticado a través de una red de comunicación móvil, y

en respuesta a dicha adquisición de la primera información de identificación personal, enviar la segunda información de identificación personal al servidor de procesamiento de datos de autenticación para completar la autenticación del terminal de procesamiento de datos.

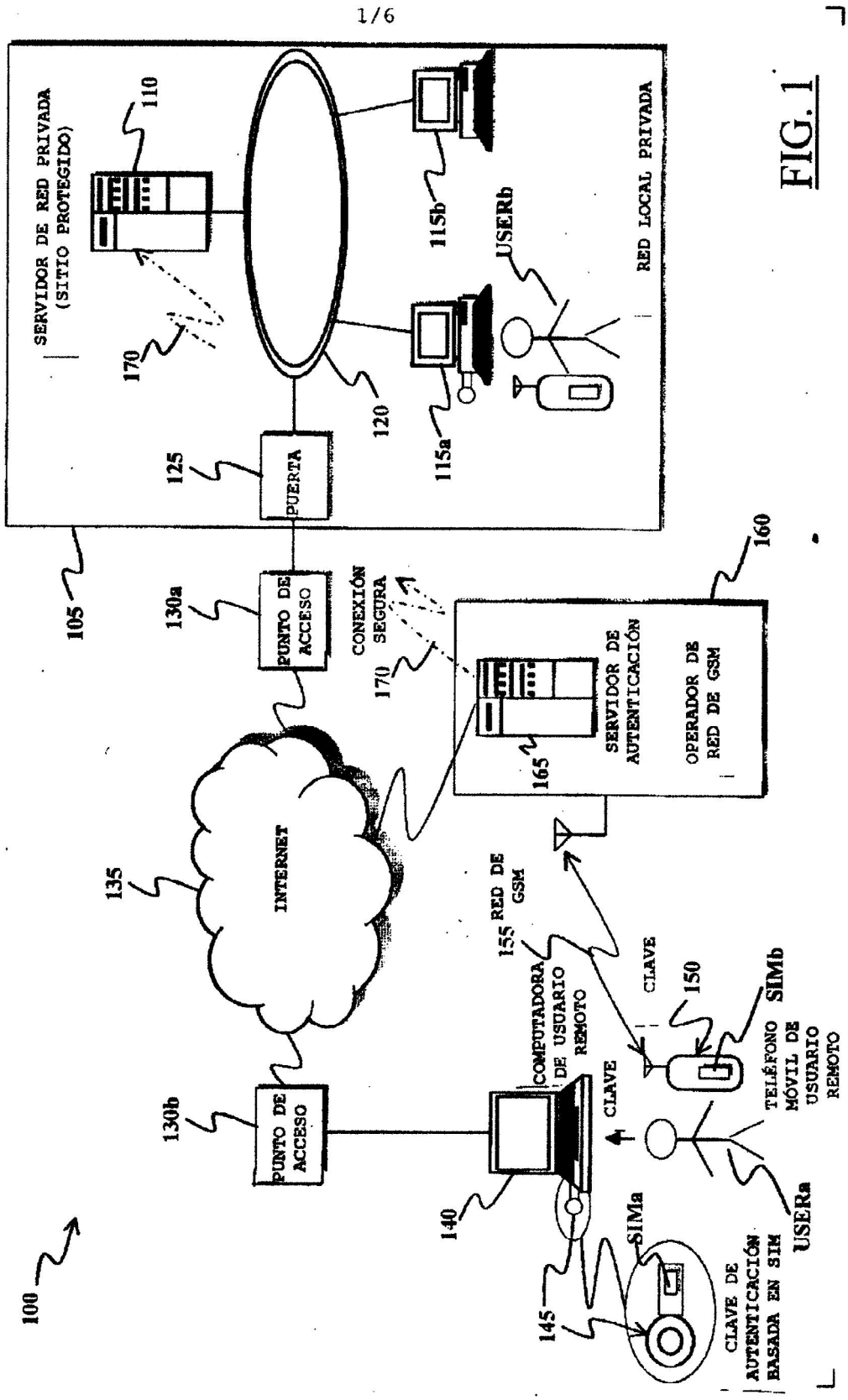
1/6
SERVIDOR DE RED PRIVADA
(SITIO PROTEGIDO)
110
170
125
PUERTA
120
115a
115b
USERb
RED LOCAL PRIVADA
105
130a
PUNTO DE ACCESO
CONEXIÓN SEGURA
170
160
SERVIDOR DE AUTENTICACIÓN
OPERADOR DE RED DE GSM
165
INTERNET
135
RED DE GSM
155
CLAVE
150
SIMb
TELÉFONO MÓVIL DE USUARIO REMOTO
USERa
130b
PUNTO DE ACCESO
COMPUTADORA DE USUARIO REMOTO
CLAVE
140
SIMa
145
CLAVE DE AUTENTICACIÓN BASADA EN SIM
100

FIG. 1

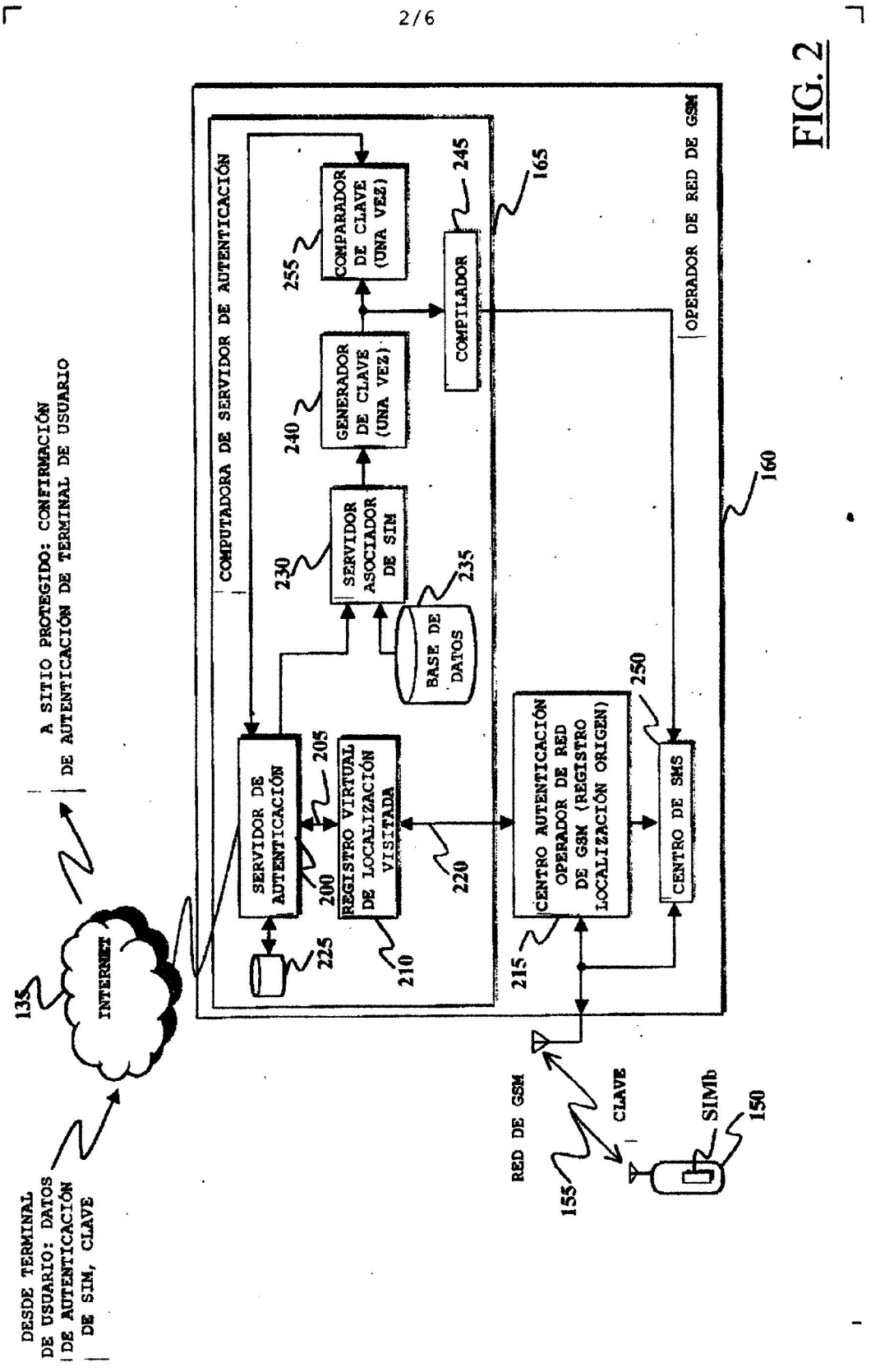
2/6
DESDE TERMINAL DE USUARIO: DATOS DE AUTENTICACIÓN DE SIM, CLAVE
A SITIO PROTEGIDO: CONFIRMACIÓN DE AUTENTICACIÓN DE TERMINAL DE USUARIO
INTERNET
135
COMPUTADORA DE SERVIDOR DE AUTENTICACIÓN
SERVIDOR DE AUTENTICACIÓN
205
200
REGISTRO VIRTUAL DE LOCALIZACIÓN VISITADA
220
225
210
SERVIDOR ASOCIADOR DE SIM
230
BASE DE DATOS
235
GENERADOR DE CLAVE (UNA VEZ)
240
COMPARADOR DE CLAVE (UNA VEZ)
255
COMPILADOR
245
165
OPERADOR DE RED DE GSM
160
CENTRO AUTENTICACIÓN OPERADOR DE RED DE GSM (REGISTRO LOCALIZACIÓN ORIGEN)
250
CENTRO DE SMS
215
RED DE GSM
155
CLAVE
SIMb
150

FIG. 2

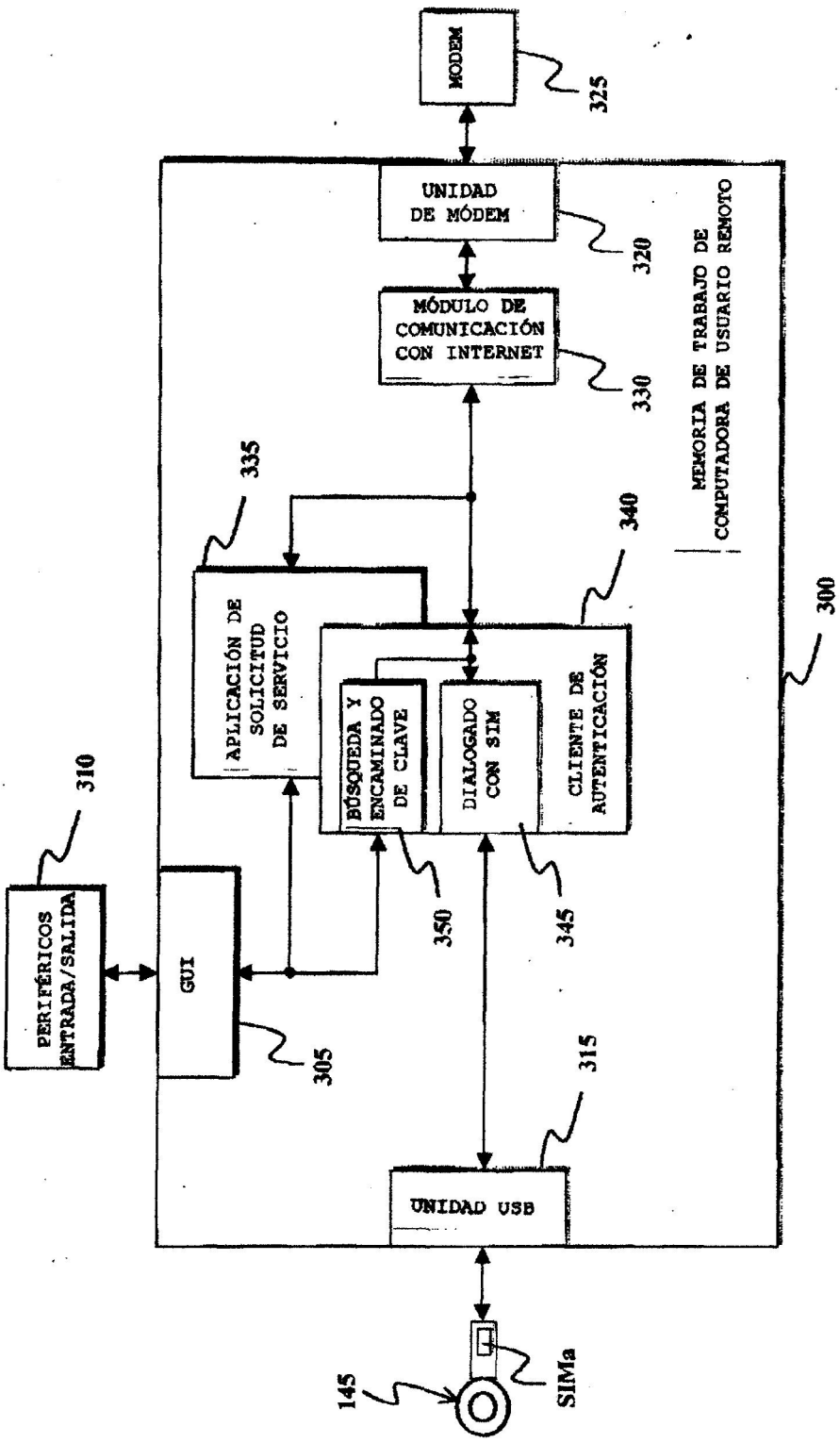
MODEM
325
UNIDAD DE MÓDEM
320
MÓDULO DE COMUNICACIÓN CON INTERNET
330
MEMORIA DE TRABAJO DE COMPUTADORA DE USUARIO REMOTO
300
335
340
APLICACIÓN DE SOLICITUD DE SERVICIO
BÚSQUEDA Y ENCAMINADO DE CLAVE
DIALOGADO CON SIM
CLIENTE DE AUTENTICACIÓN
310
PERIFÉRICOS ENTRADA/SALIDA
GUI
305
350
345
315
UNIDAD USB
145
SIMa

FIG. 3

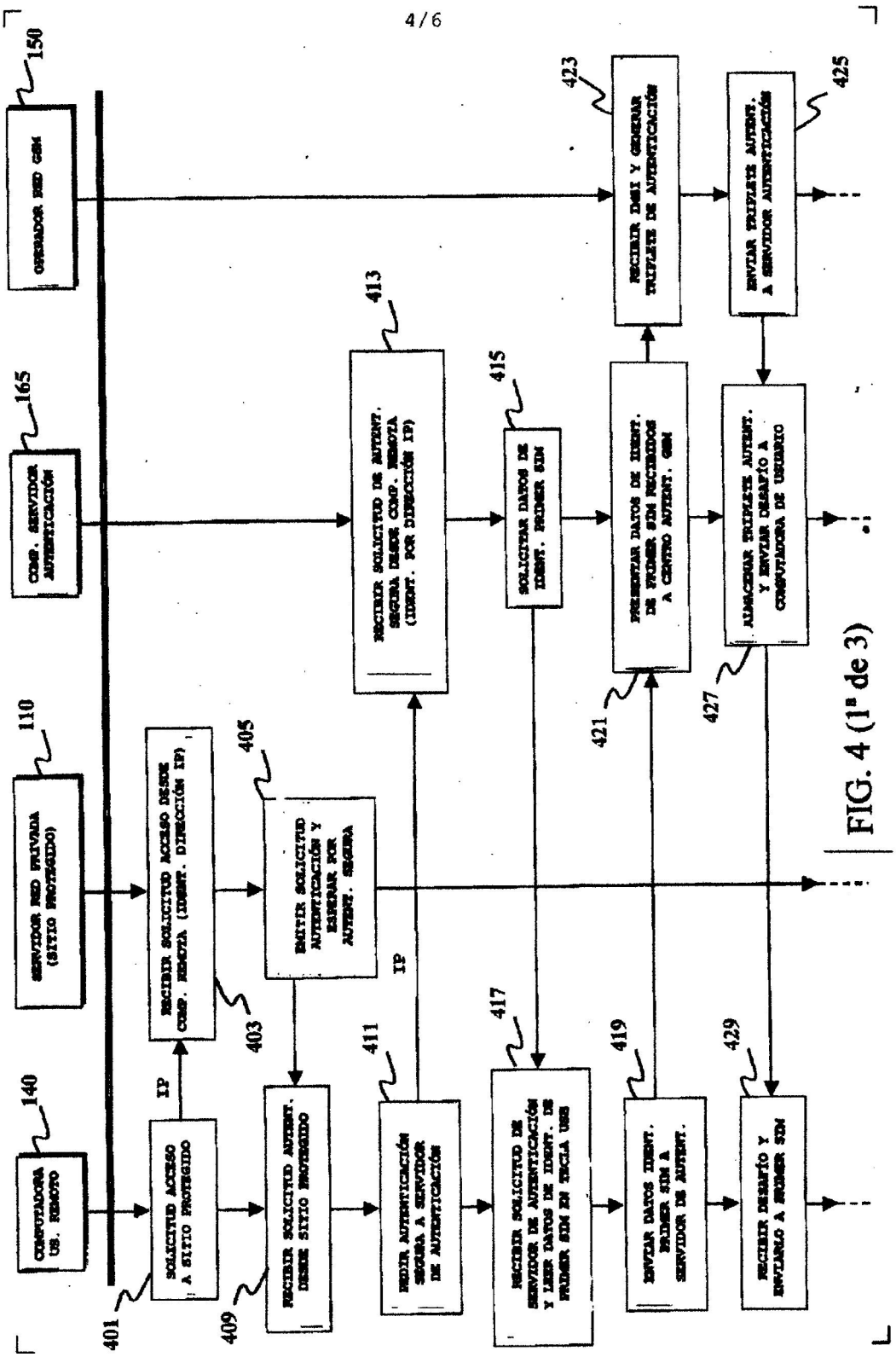
4/6
OPERADOR RED GSM
150
COMP. SERVIDOR AUTENTICACIÓN
165
SERVIDOR RED PRIVADA (SITIO PROTEGIDO)
110
ORDENADOR US. REMOTO
140
401
SOLICITUD ACCESO A SITIO PROTEGIDO
IP
409
RECIBIR SOLICITUD ACCESO DESDE COMP. REMOTA (IDENT. DIRECCIÓN IP)
403
RECIBIR SOLICITUD AUTENT. DESDE SITIO PROTEGIDO
ENVIAR SOLICITUD AUTENTICACIÓN Y ESPERAR POR AUTENT. SEGURA
405
IP
411
PEDIR AUTENTICACIÓN SEGURA A SERVIDOR DE AUTENTICACIÓN
RECIBIR SOLICITUD AUTENT. SEGURA DESDE COMP. REMOTA (IDENT. POR DIRECCIÓN IP)
413
RECIBIR SOLICITUD DE SERVIDOR DE AUTENTICACIÓN Y LEER DATOS DE IDENT. DE PRIMER SIM EN ESTA RED
417
SOLICITAR DATOS DE IDENT. PRIMER SIM
415
ENVIAR DATOS IDENT. PRIMER SIM A SERVIDOR DE AUTENT.
419
PRESENTAR DATOS DE IDENT. DE PRIMER SIM RECIBIDOS A CENTRO AUTENT. GSM
421
RECIBIR DATOS Y GENERAR TRIPLETE DE AUTENTICACIÓN
423
AUMACENAR TRIPLETE AUTENT. Y ENVIAR DESAFÍO A COMPUTADORA DE USUARIO
427
ENVIAR TRIPLETE AUTENT. A SERVIDOR AUTENTICACIÓN
425
RECIBIR DESAFÍO Y ENVIARLO A PRIMER SIM
429

FIG. 4 (1ª de 3)

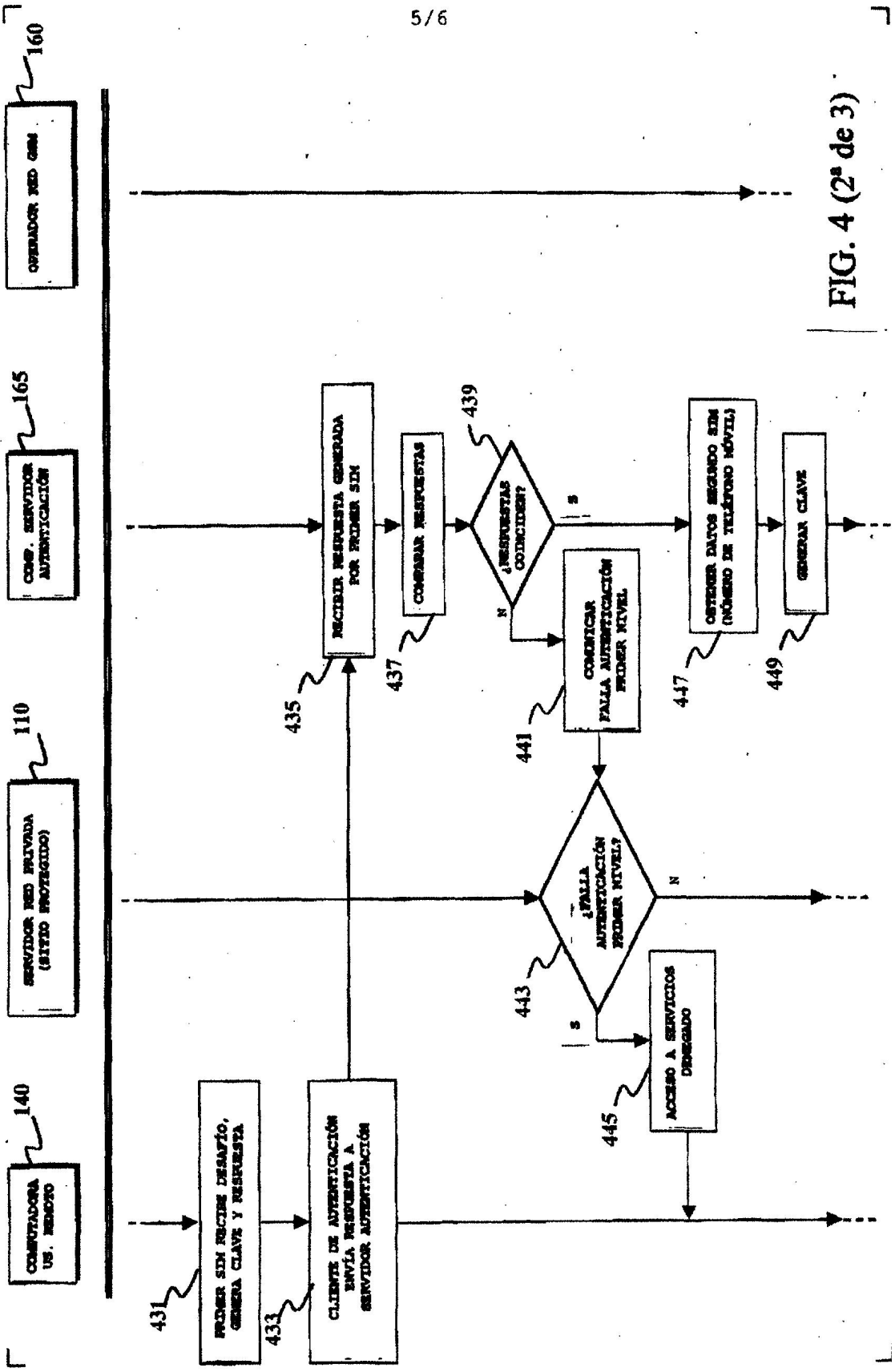
COMPUTADORA US. REMOTO
140
SERVIDOR RED PRIVADA (SITIO PROTEGIDO)
110
COMP. SERVIDOR AUTENTICACIÓN
165
OPERADOR RED GSM
160
431
PROMUEVE SIN RECIBIR DESAFÍO, GENERA CLAVE Y RESPUESTA
433
CLIENTE DE AUTENTICACIÓN ENVÍA RESPUESTA A SERVIDOR AUTENTICACIÓN
435
RECIBIR RESPUESTA GENERADA POR PRIMER SIM
437
COMPARAR RESPUESTAS
439
¿RESPUESTAS COINCIDEN?
S
N
441
CONDICIÓN FALLA AUTENTICACIÓN PRIMER NIVEL
443
¿FALLA AUTENTICACIÓN PRIMER NIVEL?
S
N
445
ACCESO A SERVICIOS DESEADO
447
OBTENER DATOS SEGUNDO SIM (NÚMERO DE TELÉFONO MÓVIL)
449
GENERAR CLAVE

FIG. 4 (2ª de 3)

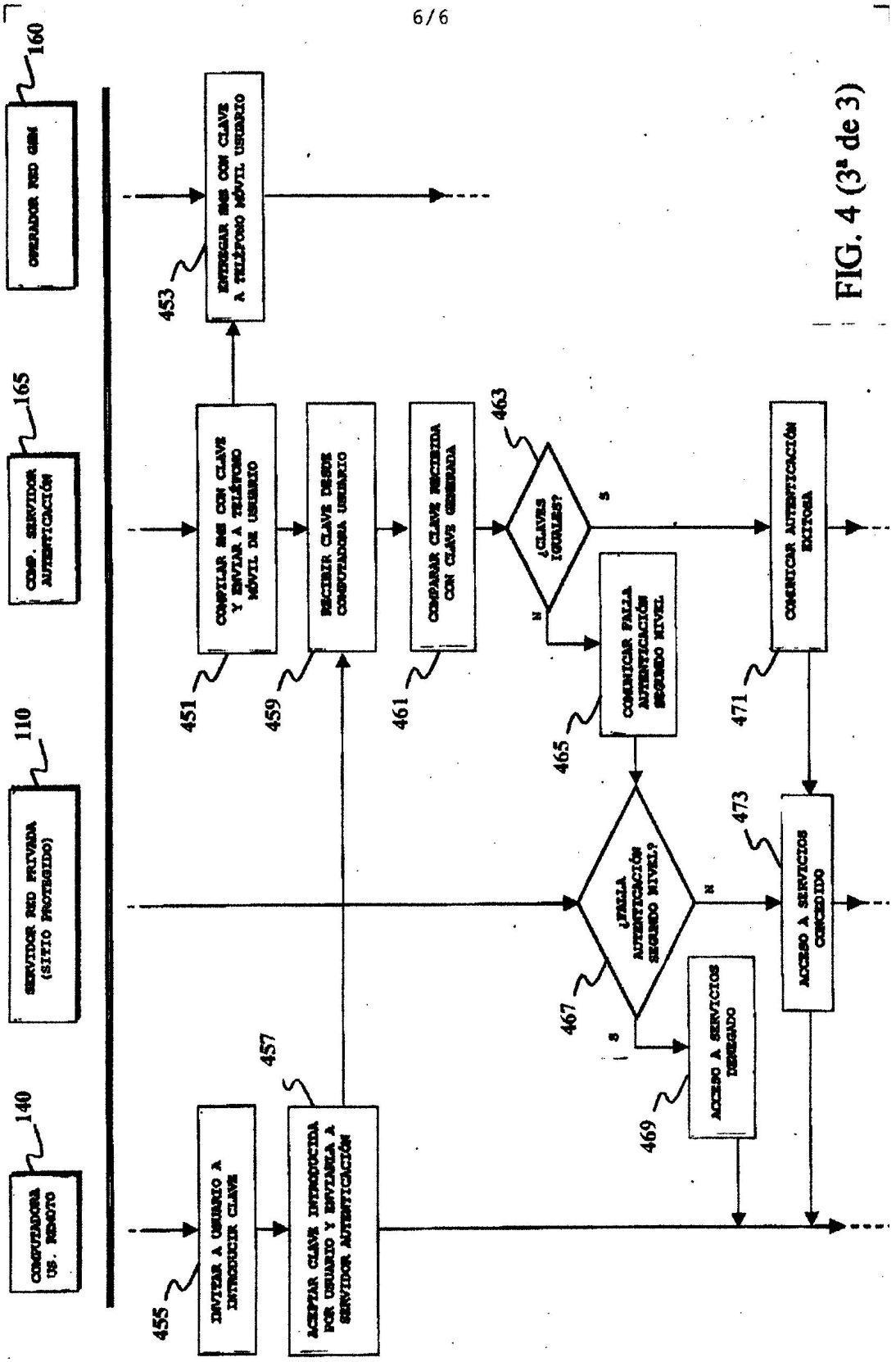
160
OPERADOR RED GSM
165
COMP. SERVIDOR AUTENTICACIÓN
110
SERVIDOR RED PRIVADA (SITIO PROTEGIDO)
140
COMPUTADORA DE USUARIO
453
ENVIAR SMS CON CLAVE A TELÉFONO MÓVIL USUARIO
451
COMPILAR SMS CON CLAVE Y ENVIAR A TELÉFONO MÓVIL DE USUARIO
459
RECIBIR CLAVE DESDE COMPUTADORA USUARIO
461
COMPARAR CLAVE RECIBIDA CON CLAVE GENERADA
463
¿CLAVES IGUALES?
S
N
465
COMUNICAR FALLA AUTENTICACIÓN SEGUNDO NIVEL
471
COMUNICAR AUTENTICACIÓN EXITOSA
467
¿FALLA AUTENTICACIÓN SEGUNDO NIVEL?
N
S
473
ACCESO A SERVICIOS CONCEDIDO
469
ACCESO A SERVICIOS DENEGADO
455
INVITAR A USUARIO A INTRODUCIR CLAVE
457
ACEPTAR CLAVE INTRODUCIDA POR USUARIO Y ENVIARLA A SERVIDOR AUTENTICACIÓN

FIG. 4 (3ª de 3)