(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 635 602**

(51) Int. CI.:

G06Q 50/18 (2012.01)
H04L 12/16 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.03.2012 PCT/CA2012/000290**

(87) Fecha y número de publicación internacional: **04.10.2012 WO12129664**

(96) Fecha de presentación y número de la solicitud europea: **30.03.2012 E 12765297 (2)**

(97) Fecha y número de publicación de la concesión europea: **21.06.2017 EP 2695136**

(54) Título: **Sistema, método, servidor y medio legible por ordenador para la verificación en tiempo real de un estado de un miembro de una organización**

(30) Prioridad:

01.04.2011 US 201161470537 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.10.2017

(73) Titular/es:

CLAWD TECHNOLOGIES INC. (100.0%)
330 rue Cormier Bureau 201
Drummondville, Québec J3C 8B3, CA

(72) Inventor/es:

MEUNIER, SEBASTIEN;
BELISLE, PIERRE y
DARTIGUES, GUY

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema, método, servidor y medio legible por ordenador para la verificación en tiempo real de un estado de un miembro de una organización

Campo técnico

La presente tecnología se refiere generalmente a sistemas informáticos y de seguridad de la información y, en particular, a técnicas criptográficas implementadas por ordenador para la autenticación y validación de usuarios que son regulados por una autoridad, un organismo regulador u otra organización.

Antecedentes

Virtualmente todas las industrias de servicios profesionales están hoy en día reguladas por autoridades de concesión de licencias profesionales u órganos de gobierno. Por ejemplo, un abogado sólo puede ejercer derecho en una jurisdicción si el colegio de abogados local ha licenciado a ese abogado. De manera similar, los contables, ingenieros, doctores médicos, dentistas, corredores de bolsa, agentes de bienes raíces, y una plétora de otros profesionales deben encontrarse en una buena situación con sus respectivas organizaciones profesionales para ser capaces de participar en la práctica de su profesión. Cuando un profesional ya no se encuentra en una buena situación con su organización profesional u órgano de gobierno, frecuentemente no existen formas fáciles para un cliente u otra parte que confía en la transacción, consejo o servicio proporcionado por el profesional de saber si el profesional en cuestión ya no tiene licencia. De manera convencional, se debe hacer una consulta formal al organismo de concesión de licencias del profesional para cerciorarse de que el profesional se encuentra en una buena situación. Esto implica esfuerzo y tiempo por lo que en la práctica frecuentemente no se hace. La situación actual deja al público expuesto a la posibilidad de que el profesional esté actuando sin una licencia válida del organismo regulador. Esto es particularmente importante para clientes que confían en profesionales tales como abogados o contables que están involucrados en transacciones electrónicas en nombre de sus clientes. Las tecnologías actuales no permiten que el estado de un miembro de una organización sea verificado en tiempo real o aproximadamente en tiempo real para asegurar que el profesional a punto de actuar en la transacción electrónica está de hecho en una buena situación y tiene así capacidad legal para actuar en la transacción electrónica.

Sería altamente deseable una solución al problema técnico anterior. Dicha solución se describe en la presente especificación y en los dibujos adjuntos.

Breve descripción de los dibujos

Características y ventajas adicionales de la presente tecnología se harán evidentes en la siguiente descripción detallada, tomada en combinación con los dibujos adjuntos, en los cuales:

La FIG. 1 es una representación esquemática de una red de ordenadores en la cual se pueden implementar las realizaciones de la presente invención para verificar el estado de un miembro de una organización;

La FIG. 2 es una representación esquemática de un sistema de acuerdo con una realización de la presente invención que emplea un servidor de autenticación y verificación y un servidor de verificación para verificar el estado de un miembro de una organización con la web de servicios de la organización; y

La FIG. 3 es un flujo de mensajes que describe un nuevo método de verificación de acuerdo con una realización de la presente invención.

Se ha de notar que en todos los dibujos adjuntos, las mismas características están definidas por los mismos números de referencia.

Compendio

La presente invención proporciona de manera general un nuevo sistema, método, y medio legible por ordenador para verificar automáticamente el estado de un miembro con una organización profesional, órgano de gobierno u otra autoridad que regula la práctica de la profesión del miembro. En general, y esto se elaborará a continuación en un mayor detalle, la presente invención usa un nuevo servidor de autenticación y verificación de estado para enviar una solicitud al servicio web de una organización profesional para determinar el estado del miembro profesional. Esta solicitud es enviada en respuesta al inicio de sesión del miembro profesional en el servidor de autenticación y verificación de estado. Tras recibir la afirmación de que el miembro profesional se encuentra en una buena situación, esto es que el estado es OK, el servidor de estado y verificación entonces genera un certificado específico de sesión para usar por el miembro profesional en la sesión actual. Cuando el usuario inicia otra sesión, se debe crear otro certificado específico de sesión. Todo lo anterior proporciona una manera innovadora de verificar que un miembro profesional se encuentra en una buena situación. Esto permite al organismo regulador profesional, a las autoridades de concesión de licencias profesionales y a otras autoridades que regulan su afiliación controlar las actividades de los miembros que no se encuentran en una buena situación, siendo esto porque han sido retirados, no pagaron sus cuotas de afiliación, han sido suspendidos por mala conducta, etc.

Un aspecto de la presente invención es un método de verificación del estado de un miembro de una organización. El método implica el envío de una solicitud de consulta de estado a un servicio web de una organización por el estado de un miembro de la organización, recibiendo una respuesta de estado del servicio web de la organización, generando un certificado específico de sesión basado en la respuesta de estado, y comunicando el certificado específico de sesión al miembro.

Otro aspecto de la presente invención es un medio legible por ordenador sobre el cual se almacenan instrucciones en código que se configuran para realizar los pasos del método anterior cuando el medio legible por ordenador es cargado en la memoria y es ejecutado en un procesador de un dispositivo informático.

Otro aspecto de la presente invención es un sistema para verificar el estado de un miembro de una organización. El sistema incluye un servidor de autenticación y verificación de estado configurado para recibir una solicitud de inicio se sesión de un dispositivo informático asociado con el miembro, un servidor de identificación conectado de manera comunicativa al servidor de autenticación y verificación de estado para recibir la información de inicio de sesión del servidor de autenticación y verificación de estado y para proporcionar las credenciales al miembro para el servidor de autenticación y verificación de estado , y un servidor web de la organización para recibir una consulta del estado, buscando el estado del miembro, y para responder con un reporte de estado del miembro en respuesta a la consulta de estado. El servidor de identificación se configura además para generar un certificado específico de sesión y comunicar el certificado específico de sesión al servidor de autenticación y verificación de estado. El servidor de autenticación y verificación de estado se configura además para comunicar el certificado específico de sesión recibido del servidor de identificación al dispositivo informático asociado al miembro.

Un aspecto adicional de la presente invención es un método para emitir un certificado, comprendiendo el método autenticar a un miembro de una organización que inicia sesión en un servidor, verificar el estado del miembro comunicando una consulta de estado desde el servidor al servidor web de la organización y recibiendo una respuesta de estado del servidor web de la organización, y generando un certificado basado en la respuesta de estado.

Un aspecto adicional de la presente invención es un medio legible por ordenador que comprende instrucciones programadas en código que, cuando son cargadas en una memoria y son ejecutadas por el procesador de un servidor, provoca que el servidor autentique a un miembro de una organización que inicia sesión en un servidor, verifique el estado del miembro comunicando la consulta de estado desde el servidor al servidor web de la organización y recibiendo una respuesta de estado desde el servidor web de la organización, y genera una certificado basado en la respuesta de estado.

Un aspecto adicional de la presente invención es un servidor de autenticación y verificación de estado que comprende una memoria operativamente acoplada a un procesador para generar un mensaje que comprende una solicitud de consulta de estado y para provocar la comunicación del mensaje a los servicios web de una organización para obtener el estado de un miembro de la organización. La memoria y el procesador se configuran además para recibir una respuesta de estado desde los servicios web de la organización, para generar un certificado específico de sesión basado en la respuesta de estado y para comunicar el certificado específico de sesión al miembro.

Los detalles y particularidades de estos aspectos de la invención se describirán ahora, a modo de ejemplo, con referencia a los dibujos adjuntos.

Descripción detallada

Las realizaciones de la presente invención, que son descritas a continuación, permiten la verificación electrónica automatizada y/o en tiempo real del estado de un miembro de una organización. Como se elaborará a continuación, esta tecnología asegura que los miembros de una organización sólo participan en transacciones electrónicas cuando se encuentra en una buena situación con la organización.

La Fig.1 es una representación esquemática de una red de ordenadores en la cual se pueden implementar las realizaciones de la presente invención para verificar el estado de un miembro de una organización.

Como se representa a modo de ejemplo en la FIG. 1, uno o más usuarios (que son miembros de una organización) se pueden autenticar y se pueden verificar sus estados cuando cada usuario inicia sesión en el sistema para realizar una transacción electrónica. Por el bien de la ilustración, se representan tres de dichos usuarios o miembros a modo de ejemplo en la FIG. 1. Estos son el Usuario1, designado por el número de referencia 10, el Usuario2, designado por el número de referencia 20, y el Usuario3, designado por el número de referencia 30. El número de usuarios/miembros mostrados en esta realización ejemplar es arbitrario y es únicamente con propósitos de ilustración. De nuevo por el bien de la ilustración, el Usuario 1 se conecta al sistema a través de Internet 50 usando un ordenador de escritorio 12, el Usuario2 se conecta al sistema a través de Internet 50 usando un ordenador portátil 22 y el Usuario3 se conecta al sistema a través de un dispositivo móvil 32 conectado de manera comunicativa a Internet a través de una red inalámbrica y una puerta de enlace. El dispositivo móvil 32 puede ser cualquier dispositivo de comunicación inalámbrico, teléfono inteligente, teléfono móvil, PDA con capacidad inalámbrica,

tableta con capacidad inalámbrica, u otro dispositivo electrónico portable o portátil que tenga capacidad de comunicación inalámbrica. El dispositivo móvil 32 se puede conectar inalámbricamente al sistema a través de una red inalámbrica (representada esquemáticamente por una torre de estación base 40) que usa cualquier tecnología móvil conocida o protocolos de comunicación tales como, por ejemplo, GSM, EDGA, LTE. CDMA. etc. Por supuesto se pueden emplear otras tecnología inalámbricas tales como, por ejemplo, Wi-Fi™, Bluetooth®, enlaces por satélite, etc. A partir de lo anterior, debería estar claro que los usuarios/miembros pueden interactuar con el sistema usando cualquier dispositivo informático con una conexión a Internet.

Como se representa a modo de ejemplo en la FIG. 1, los miembros (Usuario 1, Usuario2 y Usuario3) se conectan a través de Internet usando protocolos de comunicación estándar, tales como TCP/IP, a los servidores 60, 70 de la interfaz Web los cuales están conectados respectivamente a través de los cortafuegos 62, 72 a un servidor 80 de autenticación y verificación de estado y a un servidor 90 de bóveda de documentos y de gestión de transacciones. Como se representa en la arquitectura ejemplar mostrada en la FIG. 1, el servidor 80 de autenticación y verificación de estado y el servidor 90 de bóveda de documentos y de gestión de transacciones están ambos conectados a un servidor 100 de ID y seguridad común (de aquí en adelante referido simplemente como un “servidor de identificación”).

Brevemente, el servidor 90 de bóveda de documentos y de gestión de transacciones (que no es el foco de la presente especificación) actúa como una sala de trato o plataforma de transacciones electrónicas seguras donde los documentos pueden ser compartidos, vistos, creados, editados, eliminados, etc, o donde se pueden realizar otras actuaciones como leer, revisar, verificar, aprobar o votar, en un entorno seguro y controlado donde aquellos que acceden e interactúan con los documentos o a aquellos que votan se les han concedido derechos y privilegios específicos respecto a los documentos o la transacción. Este servidor 90 permite realizar las transacciones electrónicas de una manera criptográficamente segura donde las actuaciones realizadas por los miembros con respecto a los documentos no se pueden repudiar más tarde.

Como se representa además a modo de ejemplo en la FIG. 1, el servidor 80 de autenticación y verificación de estado se conecta a uno o más servidores web 84 de organizaciones tales como, por ejemplo, los servicios web asociados con distintas organizaciones profesionales. Cada uno de estos servidores web almacenan datos actualizados sobre el estado de cada miembro de la organización, esto es si un miembro o usuario dado se encuentra actualmente en una buena situación o no.

La FIG. 2 es una representación esquemática de un sistema de acuerdo con una realización de la presente invención que emplea un servidor 80 de autenticación y verificación y un servidor 100 de identificación para verificar el estado de un miembro de una organización con los servicios web 84 de la organización. Este esquema se presenta en conjunción con la FIG. 3 que es un flujo de mensajes que describe el método de verificación relacionado. Los pasos numerados 1-9 en la FIG. 2 corresponden con los pasos 1-9 del flujo de mensajes en la FIG. 3. Estas dos figuras se describirán por lo tanto juntas. Como se muestra a modo de ejemplo en la FIG. 2 y FIG. 3, el método comienza (en el paso 1) cuando una usuaria, llamada Alicia en este ejemplo, inicia sesión en el sistema, esto es inicia sesión en el servidor 80 de autenticación y verificación de estado. En el paso 2, el servidor 80 de autenticación y verificación de estado envía una solicitud al servidor 100 de identificación para validar el ID de Alicia. En el paso 3, el servidor de ID recupera las credenciales de Alicia y su certificado personal (esto es un certificado digital o un certificado criptográfico asociado con el miembro Alicia). La recuperación puede ser desde una memoria del servidor de identificación en sí o desde otro servidor seguro o base de datos comunicativamente conectada al servidor de identificación. Las credenciales y el certificado se pueden almacenar juntos o se pueden almacenar de manera separada (esto es en servidores separados).

Aún referente a la Fig. 2 y la FIG. 3, después de obtener las credenciales de Alicia y determinar las reglas asociadas con esas credenciales, el servidor 80 de autenticación y verificación de estado envía una solicitud en el paso 4 (esto es transmite un mensaje que contiene una consulta de estado) a los servicios Web de la organización profesional de Alicia para verificar el estado de Alicia, esto es para validar que el estado profesional de Alicia se encuentra aún en una buena situación. En muchas implementaciones, la consulta de estado es un mensaje en una forma prescrita que los servicios web pueden reconocer y procesar de manera automática para generar un reporte de estado o una respuesta electrónica automatizada. En el paso 5, el servicio web responde con un reporte de estado o respuesta de estado. En una implementación sencilla, la respuesta de estado es un OK o un no OK (NOK) binario. En implementaciones con más matices, la respuesta de estado puede contener limitaciones en los derechos o privilegios del miembro. Por ejemplo, las limitaciones pueden prescribir que el miembro puede sólo ejercer en ciertas ubicaciones geográficas, sobre transacciones que no excedan un cierto valor monetario, o sobre ciertos tipos de transacciones, etc.

Aún referente a la FIG. 2 y FIG. 3, el servidor 80 de autenticación y verificación de estado determina si la respuesta de estado es OK o NOK. Si la respuesta de estado es OK, en el paso 7, el servidor 80 de autenticación y verificación de estado envía una solicitud al servidor 100 de identificación. El servidor 100 de identificación entonces genera un testigo (o equivalente) único que se adjunta o se asocia de otra manera con la sesión actual. En el paso 8, el servidor 100 de identificación entonces crea o genera un certificado específico de sesión único (designado en la presente memoria como cert+). Este certificado específico de sesión único se puede generar mejorando criptográficamente el certificado personal, por ejemplo añadiendo otra información al certificado personal. En el paso

9, el certificado específico de sesión se comunica al servidor 80 de autenticación y verificación de estado que entonces transmite este certificado (cert+) a Alicia. Alicia puede entonces firmar electrónicamente con su certificado específico de sesión cuando ella realice transacciones o actúe en el servidor 90 de bóveda de documentos y gestión de transacciones. El certificado específico de sesión se mantiene disponible para Alicia hasta el final de su sesión. Tras la terminación de la sesión, esto es cuando Alicia cierre la sesión, el certificado específico de sesión es eliminado o retirado (y archivado). Un nuevo certificado se puede crear para Alicia para cada sesión posterior. Los mensajes enviados entre las distintas entidades se pueden encriptar usando cualquier número de técnicas de encriptación conocidas, incluyendo el establecimiento de un túnel seguro o una red privada virtual (VPN).

La tecnología descrita anteriormente es así capaz de verificar electrónicamente en tiempo real que el miembro de la organización se encuentra de hecho en una buena situación con la organización como precondición para permitir al miembro participar en una transacción electrónica o para realizar electrónicamente una actuación. Las transacciones o actuaciones (tales como aquellas realizadas en el servidor 90 de bóveda de documentos y gestión de transacciones) pueden sólo ser realizadas por el miembro una vez que ha recibido la aprobación electrónica del servidor web de la organización en forma de una respuesta de estado o una consulta de estado. Todas las actuaciones o transacciones están firmadas por el certificado específico de sesión del miembro, el cual se crea únicamente para la sesión. Ya que el certificado específico de sesión se crea en respuesta a tanto la autenticación del miembro como la verificación de estado separada con la organización del miembro, no se puede repudiar una firma digital del miembro que usa este certificado específico de sesión.

El certificado personal y el certificado específico de sesión proporcionan así la primera y segunda identidades digitales del miembro. La primera identidad digital es una identidad digital personal que únicamente identifica al miembro. La segunda identidad digital identifica además al miembro como que es miembro de la organización. Por ejemplo, en el contexto específico de un profesional que es miembro de una organización profesional, la segunda identidad digital establece no sólo quién es el profesional sino que el profesional se encuentra en una buena situación con la organización profesional. Esta segunda identidad digital se puede usar para realizar tareas digitales relacionadas profesionalmente tales como participar en transacciones en el servidor 90 de bóveda de documentos y gestión de transacciones.

Una vez que el miembro en una buena situación ha sido verificado con su organización, este miembro puede entonces verificar la identidad de una tercera parte. Esta verificación puede, por ejemplo, implicar al miembro que examina documentos de identidad, documentos de identificación personal, datos biométricos obtenidos de un sistema biométrico, etc. Una vez que el miembro es satisfecho en grado suficiente de que la tercera parte es de hecho la persona que la tercera parte pretende ser, se puede realizar el siguiente nuevo método que involucra al miembro, que usa su identidad digital profesional (por ejemplo su certificado mejorado CERT+), avalando electrónicamente la identidad de la tercera parte. El método se puede realizar, por ejemplo, creando una firma digital que usa el certificado específico de sesión del miembro (la identidad digital profesional) en conexión con la verificación de la tercera parte. En otras palabras, el miembro firma digitalmente para significar que el miembro avala la identidad de una tercera parte. En respuesta a la firma digital del miembro, se crea un nuevo certificado digital para la tercera parte. Como tal, el nuevo certificado digital creado para la tercera parte se declara o de otra manera se enlaza al certificado usado por el miembro que ha verificado la identidad de la tercera parte.

Ahora se describe una implementación más detallada de este método. En un primer paso, un miembro de la organización inicia sesión en el servidor 80 y se autentica. El inicio de sesión puede involucrar, por ejemplo, un nombre de usuario, contraseña, datos biométricos, etc. El objetivo del miembro, en este punto, es validar la identidad de una tercera parte (esto es un individuo o persona) que desea obtener su propio certificado personal. Antes de que a la tercera parte se le pueda conceder un certificado, primero el estado del miembro debe ser verificado. Esto se puede hacer, como se describió anteriormente, mediante un servicio web entre el servidor 80 y el servidor o servidores web de la organización. Como ya se describió anteriormente, se devuelve una respuesta de estado en respuesta a una consulta de estado enviada al servidor web de la organización. Esta respuesta de estado confirma si el miembro se encuentra en una buena situación con la organización. Esta confirmación puede incluir también de manera opcional información más detallada sobre el estado, rol, título o capacidad del miembro dentro de la organización. Si la respuesta de estado confirma que el miembro se encuentra en una buena situación, se genera un certificado específico de sesión. Este certificado específico de sesión es requerido por los procesos posteriores de validación de la identidad de una tercera parte. En otras palabras, la validación de la identidad de la tercera parte se enlaza a la verificación de estado del miembro que valida la identidad de la tercera parte. Sólo si el miembro se ha autenticado exitosamente y sólo si el estado del miembro se ha verificado exitosamente se puede crear un certificado específico de sesión, el cual es una precondición para la validación exitosa de la identidad de la tercera parte. Como tal, la generación del certificado específico de sesión para el miembro es una precondición para la generación de un certificado digital (certificado personal) para la tercera parte. Por consiguiente, la generación y/o uso de un certificado digital es dependiente de la emisión de un certificado específico de sesión que sólo es generado tras la finalización de un proceso a través del cual el miembro es autenticado y a través del cual el estado del miembro es verificado con el servicio web de la organización a la cual pertenece el miembro.

Lo anterior puede ser entendido también como un nuevo método de emitir un certificado (esto es un certificado digital o un certificado criptográfico) que requiere que el servidor emita el certificado para participar en un diálogo de

verificación o en un intercambio de mensajes con un servidor web de una organización para determinar primero que un miembro que solicita la autenticación se encuentra en una buena situación con la organización antes de generar un certificado para ese miembro. En otras palabras, tras la recepción una solicitud de inicio de sesión u otra solicitud de autenticación de un miembro de una organización, el servidor automáticamente desencadena un proceso de verificación de estado con un servidor web externo controlado por la organización. Tras la recepción de una confirmación del estado del miembro, se genera un certificado para el miembro. Este método puede ser implementado por un servidor de emisión de certificados o por cualquier otro dispositivo informático que lea código de un medio legible por ordenador.

Cada uno de los servidores descritos anteriormente puede ser una máquina servidora única o un grupo de servidores. La tecnología anterior se puede implementar también en la nube. Cada servidor descrito en las figuras puede incluir uno o más procesadores (o microprocesadores), una memoria, uno o más puertos de comunicaciones y dispositivos de entrada/salida. Debería ser entendido que el sistema representado en las figuras es ejemplar. Las funciones que se muestran como que son realizadas por separado y en distintos servidores pueden, en otras implementaciones, ser realizadas por un único servidor.

Cualquiera de los métodos descritos en la presente memoria se puede implementar en hardware, software, firmware o cualquier combinación de los mismos. Cuando se implementa como software, los pasos del método, actuaciones u operaciones se pueden programar o codificar como instrucciones legibles por ordenador y se pueden registrar electrónicamente, magnéticamente u ópticamente en un medio legible por ordenador no transitorio, en una memoria legible por ordenador, en una memoria legible por una máquina o en un producto programa informático. En otras palabras, la memoria legible por ordenador o el medio legible por ordenador comprende las instrucciones en código las cuales al ser cargadas en una memoria y ser ejecutadas por un procesador de un dispositivo informático provocan que el dispositivo informático realice uno o más del método o métodos anteriores.

Un medio legible por ordenador puede ser cualquier medio que contenga, almacene, se comunique, propague o transporte el programa para su uso por o en conexión con el sistema, aparato o dispositivo de ejecución de instrucciones. El medio legible por ordenador puede ser electrónico, magnético, óptico, electromagnético, de infrarrojos o cualquier sistema o dispositivo semiconductor, Por ejemplo, el código ejecutable por ordenador para realizar los métodos descritos en la presente memoria puede ser registrado de manera tangible en un medio legible por ordenador que incluye, pero no se limita a, un disco volátil, un CD-ROM, un DVD, RAM, ROM, EPROM, Memoria Flash o cualquier tarjeta de memoria adecuada, etc. El método puede también ser implementado en hardware, Una implementación de hardware puede emplear circuitos de lógica discreta que tienen puertas lógicas para implementar funciones lógicas en las señales de datos, un circuito integrado para aplicaciones específicas (ASIC) que tiene puertas lógicas combinadas apropiadas, una matriz de puertas programables (PGA), una matriz de puertas programables en campo (FPGA), etc.

El ejemplo anterior se refiere a organizaciones profesionales tales como organismos de concesión de licencias profesionales u otras de tales autoridades. Sin embargo, esta tecnología se puede aplicar a cualquier organización que mantenga un registro web de sus miembros que se pueda consultar para determinar el estado de un miembro dado.

Esta invención se ha descrito en términos de realizaciones, implementaciones y configuraciones específicas que están destinadas a ser sólo ejemplares. Las personas de habilidad ordinaria en la técnica apreciarán, habiendo leído esta descripción, que se pueden hacer muchas variaciones, modificaciones y refinamientos obvios sin salir del concepto o conceptos inventivos presentados en la presente memoria. El ámbito de aplicación del derecho exclusivo solicitado por el demandante o demandantes está destinado por lo tanto, únicamente a las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método de verificación del estado de un miembro de una organización, comprendiendo el método:

enviar una solicitud de consulta de estado a unos servicios web (84) de una organización por el estado de un miembro de la organización;

recibir una respuesta de estado de los servicios web (84) de la organización;

generar un certificado específico de sesión basado en la respuesta de estado;

comunicar el certificado específico de sesión al miembro; y

generar un certificado digital para una tercera parte usando el certificado específico de sesión como una precondición para genera el certificado digital para la tercera parte, en donde el certificado digital de la tercera parte se enlaza al certificado específico de sesión del miembro.

2. El método como se reivindica en la reivindicación 1 en donde el envío de la consulta de estado es desencadenado por el inicio de sesión del miembro en un servidor (80) de autenticación y verificación de estado.

3. El método como se reivindica en la reivindicación 1 en donde la generación del certificado específico de sesión comprende:

obtener un certificado personal asociado con el miembro; y

mejorar criptográficamente el certificado personal con información adicional para generar el certificado específico de sesión.

4. El método como se reivindica en la reivindicación 2 comprendiendo además:

recibir información de ID del miembro cuando el miembro inicia sesión en el servidor (80) de autenticación y verificación de estado; y

comunicar la información de ID a un servidor (100) de identificación para validar la información de ID.

5. El método como se reivindica en la reivindicación 4 en donde el envío de la consulta de estado comprende:

obtener las credenciales y un certificado personal del servidor (100) de identificación para el miembro; y

identificar los servicios web para la organización asociada con el miembro basados en las credenciales; y

generar un mensaje que comprende la consulta de estado.

6. El método como se reivindica en la reivindicación 1 comprendiendo además:

recibir una firma digital creada por el miembro usando el certificado específico de sesión que pertenece al miembro para significar que el miembro ha verificado la identidad de la tercera parte; y

en donde la generación del certificado digital para la tercera parte es en respuesta a la recepción de la firma digital del miembro.

7. Un sistema para verificar el estado de un miembro de una organización, comprendiendo el sistema:

un servidor (80) de autenticación y verificación de estado configurado para recibir una solicitud de inicio de sesión de un dispositivo informático (12, 22, 32) asociado con el miembro;

un servidor (100) de identificación comunicativamente conectado al servidor (80) de autenticación y verificación de estado y estando configurado para recibir información de inicio de sesión desde el servidor (80) de autenticación y verificación de estado y para proporcionar las credenciales del miembro al servidor (80) de autenticación y verificación de estado.

un servidor web (84) de la organización configurado para recibir una consulta de estado, para buscar el estado del miembro, y para responder con un reporte de estado del miembro en respuesta a la consulta de estado;

en donde el servidor (100) de identificación se configura además para generar un certificado específico de sesión y para comunicar el certificado específico de sesión al servidor (80) de autenticación y verificación de estado;

en donde el servidor (80) de autenticación y verificación de estado se configura además para comunicar el certificado específico de sesión recibido del servidor (100) de identificación al dispositivo informático (12, 22, 32) asociado con el miembro; y

en donde el servidor (100) de identificación se configura para generar un certificado digital para una tercera parte usando el certificado específico de sesión como una precondición para generar el certificado digital para la tercera parte, en donde el certificado digital de la tercera parte se enlaza al certificado específico de sesión del miembro.

8. El sistema como se reivindica en la reivindicación 7 en donde el servidor de identificación se configura para generar el certificado específico de sesión mejorando criptográficamente el certificado personal asociado con el miembro.

9. El sistema como se reivindica en la reivindicación 8 en donde el servidor (100) de identificación se configura para generar un testigo único asociado con una sesión.

10. El sistema como se reivindica en la reivindicación 7 en donde el servidor (80) de autenticación y verificación de estado se configura para obtener una confirmación con fecha y hora del servidor web de la organización y provoca que se almacena la confirmación.

11. Un medio legible por ordenador que comprende instrucciones programadas en código las cuales, cuando son cargadas en memoria y son ejecutadas por un procesador de un servidor (80) de autenticación y verificación de estado, provocan que el servidor:

envíe un solicitud de consulta de estado a un servicio web (84) de una organización por el estado de un miembro de la organización;

reciba una respuesta de estado del servicio web (84) de la organización ;

genere un certificado específico de sesión basado en la respuesta de estado;

comunique el certificado específico de sesión al miembro; y

genere un certificado digital para una tercera parte que usa el certificado específico de sesión como una precondición para generar el certificado digital para la tercera parte, en donde el certificado digital de la tercera parte se enlaza al certificado específico de sesión del miembro.

12. El medio legible por ordenador como se reivindica en la reivindicación 11 en donde el código se configura además para provocar que el servidor (80) de autenticación y verificación de estado obtenga un certificado personal asociado con el miembro de un servidor (100) de identificación, y en donde el certificado específico de sesión se genera basado en el certificado personal.

13. El medio legible por ordenador como se reivindica en la reivindicación 11 en donde el código se configura para provocar que el servidor (80) de autenticación y verificación de estado recupere las credenciales desde un servidor (100) de autenticación e identifique basado en la credenciales los servicios web (84) de la organización a la cual el miembro pertenece.

14. Un servidor (80) de autenticación y verificación de estado que comprende:

una memoria operativamente acoplada a un procesador para generar un mensaje que comprende una solicitud de consulta de estado y para provocar la comunicación del mensaje a un servicio web (84) de la organización para obtener el estado del miembro de la organización;

en donde la memoria y el procesador se configuran además para recibir una respuesta de estado desde los servicios web (84) de la organización, para provocar que se genere un certificado específico de sesión basado en la respuesta de estado y para provocar que se genere un certificado digital para una tercera parte usando el certificado específico de sesión como una precondición para generar el certificado digital, en donde el certificado digital se enlaza al certificado específico de sesión, y para comunicar el certificado específico de sesión al miembro.

15. El servidor como se reivindica en la reivindicación 14 en donde la memoria y el procesador cooperan para obtener un certificado personal asociado con el miembro de un servidor de identificación (100), siendo usado el certificado personal para generar el certificado específico de sesión.

16. El servidor como se reivindica en la reivindicación 14 en donde la memoria y el procesador cooperan para recuperar las credenciales desde un servidor (100) de identificación y para identificar basado en las credenciales los servicios web (84) de la organización a la cual pertenece el miembro.

17. Un método de emisión de un certificado, comprendiendo el método:

autenticar un miembro de una organización que inicia sesión en un servidor;

verificar el estado del miembro comunicando una consulta de estado desde el servidor hasta el servidor web (84) de la organización y recibiendo una respuesta de estado desde el servidor web (84) de la organización;

generar un certificado para el miembro basado en la respuesta de estado; y

generar un certificado digital para una tercera parte basado en el certificado del miembro después de recibir una firma digital usando el certificado del miembro firmando la verificación de la identidad de la tercera parte por el miembro.

18. El método como se reivindica en la reivindicación 17 en donde el certificado es un certificado específico de sesión.

19. Un medio legible por ordenador que comprende instrucciones programadas en código las cuales, cuando son cargadas en memoria y son ejecutadas por un procesador de un servidor, provocan que el servidor:

autentique un miembro de una organización que inicia sesión en un servidor;

verifique el estado del miembro comunicando un consulta de estado desde el servidor a un servidor web (84) de la organización y recibiendo una respuesta de estado desde el servidor web de la organización;

genere un certificado para el miembro basado en la respuesta de estado; y

genere un certificado digital para una tercera parte basado en el certificado del miembro después de recibir una firma digital usando el certificado del miembro firmando la verificación de la identidad de la tercera parte por el miembro.

20. El medio legible por ordenador como se reivindica en la reivindicación 19 en donde el certificado es un certificado específico de sesión.

21. Un servidor para emitir un certificado, comprendiendo el servidor una memoria operativamente acoplada a un procesador para provocar que el servidor:

autentique un miembro de una organización que inicia sesión en un servidor;

verifique el estado del comunicando un consulta de estado desde el servidor a un servidor web (84) de la organización y recibiendo una respuesta de estado desde el servidor web (84) de la organización; y

genere un certificado para el miembro basado en la respuesta de estado; y

genere un certificado digital para una tercera parte basado en el certificado del miembro después de recibir una firma digital usando el certificado del miembro firmando la verificación de la identidad de la tercera parte por el miembro.

22. El servidor como se reivindica en la reivindicación 21 en donde el certificado es un certificado específico de sesión.

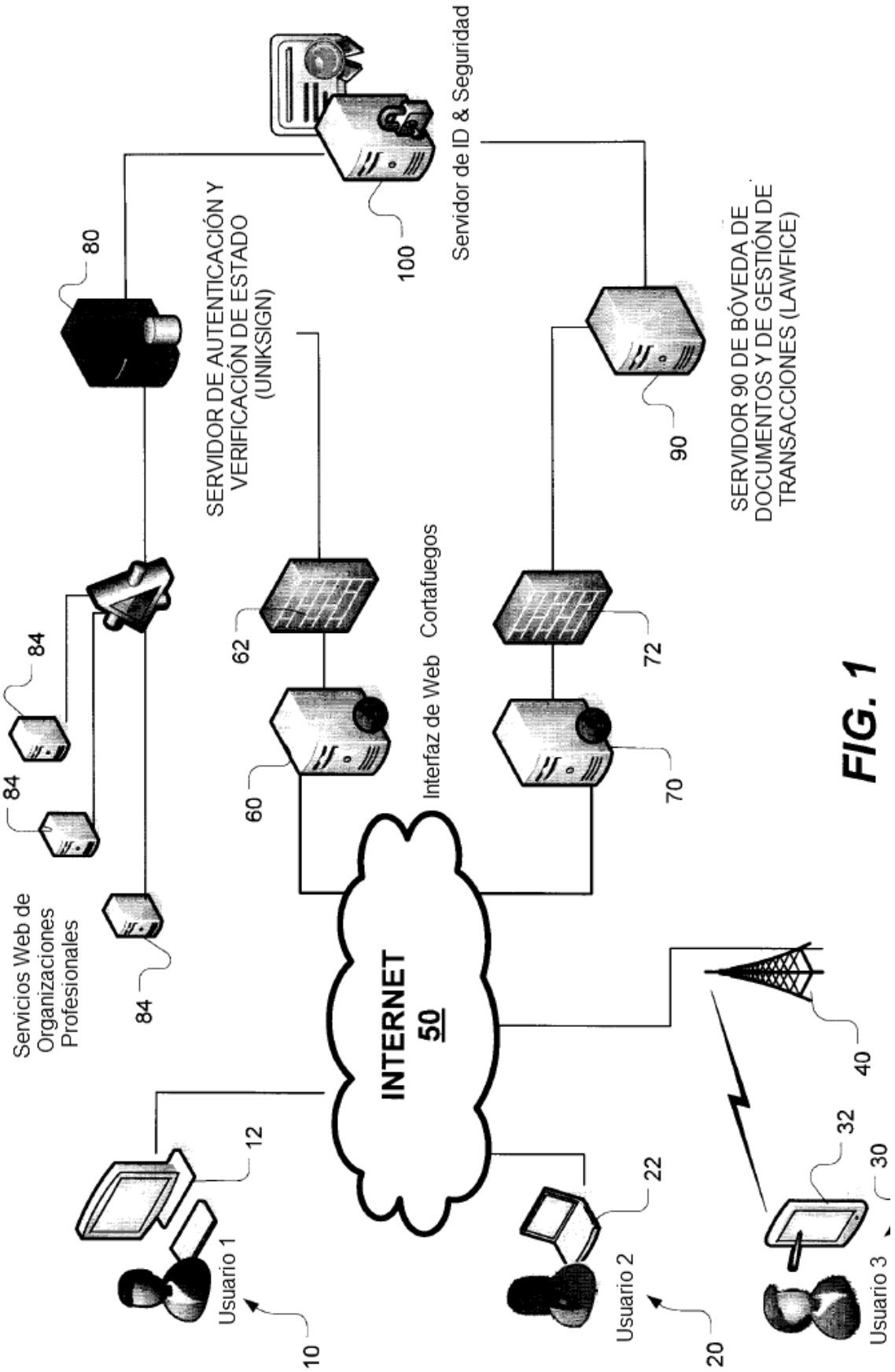
Servicios Web de Organizaciones Profesionales
84
84
84
80
SERVIDOR DE AUTENTICACIÓN Y VERIFICACIÓN DE ESTADO (UNIKSIGN)
62
60
Interfaz de Web
Cortafuegos
INTERNET
50
100
Servidor de ID & Seguridad
72
70
90
SERVIDOR 90 DE BÓVEDA DE DOCUMENTOS Y DE GESTIÓN DE TRANSACCIONES (LAWFICE)
12
Usuario 1
10
22
Usuario 2
20
40
32
30
Usuario 3

FIG. 1

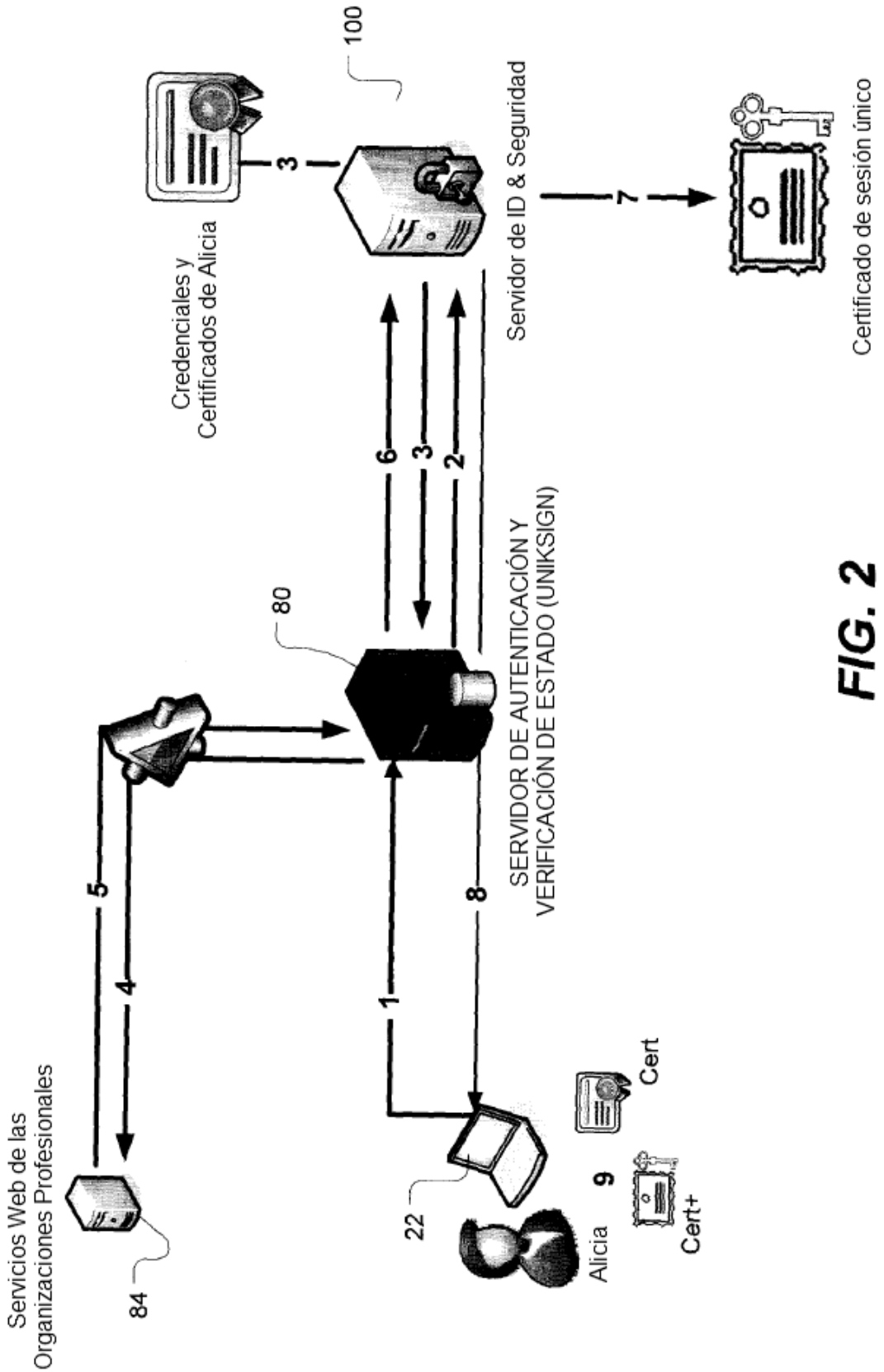
100
Credenciales y Certificados de Alicia
3
Servidor de ID & Seguridad
7
Certificado de sesión único
6
3
2
80
SERVIDOR DE AUTENTICACIÓN Y VERIFICACIÓN DE ESTADO (UNIKSIGN)
5
4
1
8
Servicios Web de las Organizaciones Profesionales
84
22
Alicia
9
Cert
Cert+

FIG. 2

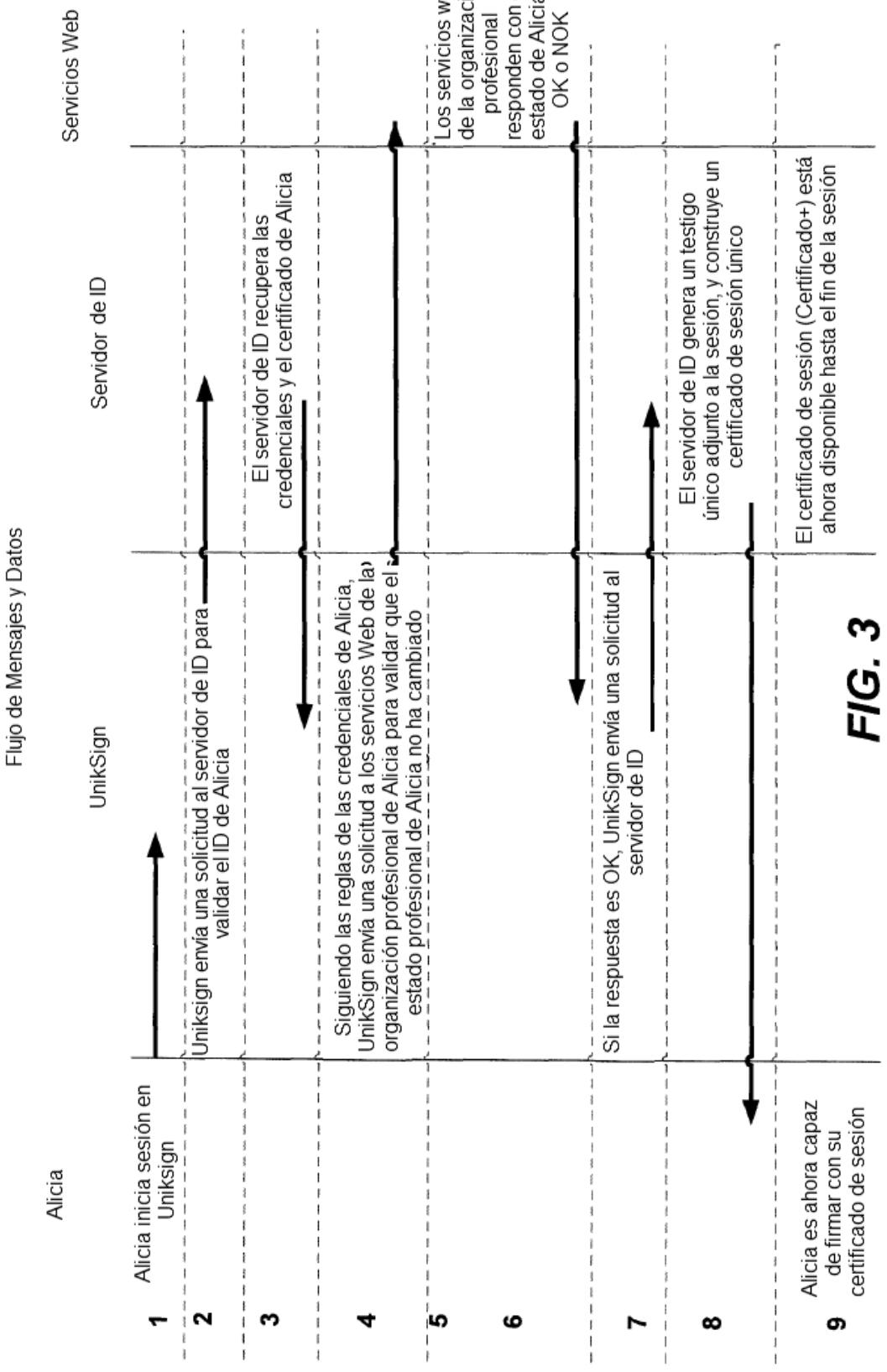
Flujo de Mensajes y Datos
Alicia
UnikSign
Servidor de ID
Servicios Web
1
Alicia inicia sesión en Uniksign
2
Uniksign envía una solicitud al servidor de ID para validar el ID de Alicia
3
El servidor de ID recupera las credenciales y el certificado de Alicia
4
Siguiendo las reglas de las credenciales de Alicia, UnikSign envía una solicitud a los servicios Web de la organización profesional de Alicia para validar que el estado profesional de Alicia no ha cambiado
5
Los servicios web de la organización profesional responden con el estado de Alicia: OK o NOK
6
Si la respuesta es OK, UnikSign envía una solicitud al servidor de ID
7
El servidor de ID genera un testigo único adjunto a la sesión, y construye un certificado de sesión único
8
El certificado de sesión (Certificado+) está ahora disponible hasta el fin de la sesión
9
Alicia es ahora capaz de firmar con su certificado de sesión

FIG. 3