(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 825 060**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
G06F 21/34 (2013.01)
G06F 21/62 (2013.01)
G06F 16/9535 (2009.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.12.2013 PCT/EP2013/077613**

(87) Fecha y número de publicación internacional: **26.06.2014 WO14096325**

(96) Fecha de presentación y número de la solicitud europea: **20.12.2013 E 13814132 (0)**

(97) Fecha y número de publicación de la concesión europea: **29.07.2020 EP 2936768**

(54) Título: **Un sistema y un método de emisión dinámica de credenciales de preservación de privacidad**

(30) Prioridad:

21.12.2012 EP 12306655

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.05.2021

(73) Titular/es:

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

(72) Inventor/es:

LU, HONGQUIAN, KAREN;
CASTILLO, LAURENT y
SMADJA, PHILIPPE

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Un sistema y un método de emisión dinámica de credenciales de preservación de privacidad

Antecedentes de la invención

La presente invención se refiere en general a la seguridad digital, y más particularmente a la creación dinámica de credenciales digitales preservadoras de privacidad.

La proliferación de servicios en línea a través de internet ha brindado a los usuarios muchas oportunidades interesantes para el comercio electrónico, las redes sociales, la computación en la nube, el archivo de datos de usuario, correo electrónico, etc. Muchos de estos servicios tratan con datos muy privados y sensibles. Esta información puede incluir números y saldos de cuentas, detalles privados de la vida de un usuario, etc. El acceso seguro a sitios web, canales de comunicación seguros, encriptación y políticas de contraseñas seguras sirven para proteger dicha información.

Sin embargo, no son solo los datos en sí los que un usuario puede considerar privados, sino también la identidad del usuario y las actividades en línea. Por ejemplo, una persona puede querer acceder a un sitio web destinado únicamente a determinadas categorías de usuarios y, al hacerlo, demostrar que es miembro de una categoría calificada sin revelar su identidad. Además, es posible que desee mantener en privado el hecho de que está visitando un sitio web en particular de terceros.

Las soluciones de identidad federada están destinadas a aliviar los inconvenientes para las personas que deben administrar el número cada vez mayor de contraseñas en los sitios web, permitir colaboraciones entre dominios y mejorar la seguridad de la administración de identidades. Sin embargo, el logro de estos objetivos para mayor comodidad de los usuarios a menudo se realiza a costa de la privacidad del usuario. Un proveedor de identidad de terceros, es decir, el tercero que actúa para verificar la identidad de un usuario en un sitio web de un proveedor de servicios al que un usuario busca acceder, puede aprender y rastrear los comportamientos de sus usuarios, como dónde y cuándo han visitado sitios particulares e incluso su actividad en esos sitios. Para los proveedores de identidad de internet, este suele ser el mecanismo principal con el que monetizar los servicios de identidad que brindan y es el núcleo de sus ofertas. El proveedor de identidad puede divulgar más información personal de la necesaria a los proveedores de servicios sin que los usuarios se den cuenta de dicha divulgación.

Los sistemas de credenciales anónimas (o credenciales preservadoras de privacidad), como U-Prove de Microsoft e Identity Mixer (Idemix) de IBM, permiten la autenticación y el control de acceso a la vez que protegen la privacidad de los usuarios. Para ello, estos sistemas evitan la vinculación de la emisión y el uso de credenciales y permiten la divulgación selectiva de información en las credenciales. Por ejemplo, se puede usar una credencial preservadora de privacidad para probar un atributo particular de un usuario, por ejemplo, la edad del usuario, sin revelar la identidad real de un usuario. Incluso si el proveedor de identidad y los proveedores de servicios coluden, no pueden rastrear el comportamiento del usuario. La criptografía proporciona una base sólida tanto para U-Prove como para Idemix. Sin embargo, la integración efectiva de las tecnologías en el ecosistema de identidad con seguridad, privacidad y usabilidad sigue siendo un desafío.

En un escenario, un usuario puede querer acceder a un proveedor de servicios (SP) a través de internet y también desear proteger su privacidad al mismo tiempo. Un proveedor de servicios (SP) es un sitio web que proporciona algún tipo de servicio a un usuario, por ejemplo, comercio electrónico, computación en la nube o redes sociales. Para permitir el acceso al servicio, el SP solicita al usuario que presente una credencial emitida por un emisor de credenciales de confianza, también conocido como proveedor de identidad (IdP). Si el usuario ya tiene la credencial, puede presentar la credencial con divulgación selectiva y otras características de protección de la privacidad. Sin embargo, si el usuario no tiene la credencial, debe obtenerla de alguna manera. Para una mejor experiencia de usuario, el SP puede indicarle al usuario que obtenga la credencial de forma dinámica y vuelva a visitar el SP después de que se haya obtenido la credencial. El uso de protocolos de federación de identidad existentes proporciona seguridad y una experiencia de usuario sin interrupciones, pero al mismo tiempo su uso anula el propósito de la credencial preservadora de privacidad porque el IdP puede aprender de qué SP proviene el usuario.

Microsoft Corporation proporciona la tecnología de credencial preservadora de privacidad U-Prove. Especificación criptográfica U-Prove, V1.1, C. Paquin, Microsoft, febrero de 2011. Microsoft ha demostrado un mecanismo para usar un Agente de U-Prove para abordar las preocupaciones mencionadas anteriormente.

Un Agente de U-Prove proporciona un mecanismo para separar la recuperación de información de organizaciones de confianza de la liberación de esta información al sitio web de destino. Documento técnico de U-Prove CTP R2, Rev. 17, J. Brown, P. Stradling, C.H. Wittenberg, Microsoft, febrero, 2011.

La criptografía subyacente de U-Prove evita que las organizaciones emisoras rastreen dónde o cuándo el usuario usa esta información. El Agente de U-Prove está compuesto por un servicio alojado en la nube y componentes de cliente opcionales. El Agente (incluidos los componentes del cliente) actúa en nombre del usuario para:

1. Interactuar con el emisor de credenciales para generar un token U-Prove y

2. Calcular una prueba de presentación y enviar el token de presentación al proveedor de servicios.

Un inconveniente de este enfoque es que el Agente de U-Prove aprende muchos detalles; el Agente de U-Prove puede rastrear desde qué proveedor de servicios el usuario ha utilizado una credencial, en qué momento ocurrió dicho uso, qué credencial se utilizó, quién emitió la credencial, etc. Proporcionar al Agente de U-Prove tanta información, en algún aspecto, ha frustrado el propósito de la credencial preservadora de privacidad.

La publicación de solicitud de patente de EE. UU. US2008/0263649 A1 divulga un token personal y un método para autenticación controlada.

La publicación de solicitud de patente de EE. UU. US2010/355441 A1 divulga un método de acceso anónimo y seudónimo flexible que preserva la privacidad.

A partir de lo anterior, resultará evidente que todavía existe la necesidad de un método mejorado para proporcionar una emisión dinámica de credenciales de usuario que no revelen la identidad de un usuario y que no revelen el comportamiento del usuario en sus actividades en línea. Para ello, la presente invención propone un método para autenticar a un usuario como se define en la reivindicación 1.

Según otro aspecto de la invención, la solicitud para generar una credencial puede estar precedida por la operación del proveedor de servicios para solicitar al usuario una prueba de un atributo; puede comprender además transmitir un mensaje de estado emitido por token desde el proveedor de identidad a la aplicación web; operar el ordenador anfitrión para redirigir el mensaje de estado emitido por token al separador; operar el separador para redirigir el mensaje de estado emitido por token al proveedor de servicios a través del ordenador anfitrión; y en donde la etapa de operar el dispositivo de seguridad para crear un token de presentación a partir de la credencial preservadora de privacidad puede ir precedida por operar el proveedor de servicios, en respuesta a recibir el mensaje de estado emitido por token, para repetir la solicitud de prueba de un atributo del usuario.

Según otro aspecto de la invención, puede comprender además operar el proveedor de servicios para verificar el token de presentación y proporcionar acceso al servicio del proveedor de servicios.

Según otro aspecto de la invención, puede comprender además operar el dispositivo de seguridad para almacenar la credencial preservadora de privacidad o el token de presentación.

Según otro aspecto de la invención, el dispositivo de seguridad puede ser una tarjeta inteligente.

Según otro aspecto de la invención, la credencial puede ser una credencial preservadora de privacidad U-Prove.

Según otro aspecto de la invención, la credencial puede ser una credencial de Identity Mixer (idemix) y el token de presentación puede ser una transformación de la credencial de idemix.

La invención también proporciona un sistema como se define en la reivindicación 8.

Breve descripción de los dibujos

La Figura 1 es una ilustración esquemática de aspectos de hardware de una red que conecta un ordenador anfitrión con un dispositivo de seguridad portátil, por ejemplo, una tarjeta inteligente, conectada a la misma, a uno o más ordenadores servidores remotos en un ecosistema de identidad.

La Figura 2 es una ilustración esquemática de programas de software correspondientes a los nodos de hardware de la Figura 1.

La Figura 3 es una ilustración esquemática de un dispositivo de seguridad 109, por ejemplo, una tarjeta inteligente.

La Figura 4 es un diagrama de bloques que ilustra ciertos programas de software cargados en el dispositivo de seguridad de la Figura 3.

La Figura 5 es un diagrama de bloques que ilustra la emisión y el uso de una credencial preservadora de privacidad.

La Figura 6 es un diagrama de secuencia temporal que ilustra el flujo de datos en un escenario previo a emisión.

La Figura 7 es un diagrama de secuencia temporal que ilustra el uso de una credencial y un token de presentación generada a partir de la misma.

La Figura 8 es un diagrama de secuencia temporal que ilustra un método que implica redirecciones dobles de la solicitud de token del proveedor de servicios a través de un separador.

Las Figuras 9a - 9d ilustran una secuencia de posibles pantallas de interacción de navegador web que indican la interacción de usuario durante redirecciones dobles como se establece en la Figura 8.

Descripción detallada de la invención

En la siguiente descripción detallada, se hace referencia a los dibujos adjuntos que muestran, a modo de ilustración, realizaciones específicas en las que se puede practicar la invención. Estas realizaciones se describen con suficiente detalle para permitir a los expertos en la técnica poner en práctica la invención. Debe entenderse que las diversas realizaciones de la invención, aunque diferentes, no son necesariamente mutuamente excluyentes. En la siguiente descripción, varios elementos relacionados se denominan n-E, n-C y n-S, respectivamente. E significa entidad, C, computadora u ordenador y S, software. Así, n-E es la entidad n-E, que opera el ordenador n-C, que se ejecuta de acuerdo con las instrucciones n-S. Por ejemplo, el proveedor de servicios 115-E opera un ordenador 115-C que ejecuta un servicio web 115-S. Para facilitar la descripción, a veces se hace referencia a estos elementos con el número n, por ejemplo, proveedor de servicios 115. A menos que el contexto indique claramente lo contrario, esto debería interpretarse normalmente en el sentido de que una referencia a los tres elementos que realizan sus funciones respectivas, por ejemplo, que el ordenador 115-C del proveedor de servicios realiza alguna acción prescrita por el software en el programa de servicios web 115-S.

En una realización de la invención, se describe un método y un sistema que proporcionan el uso de credenciales preservadoras de privacidad, por ejemplo, como las proporcionan U-Prove o Idemix, sin revelar a los proveedores de identidad cómo el usuario pretende usar la credencial preservadora de privacidad proporcionada a través del proveedor de identidad.

La Figura 1 es una ilustración esquemática de aspectos de hardware de una red 111 que conecta un ordenador anfitrión 103-C con un dispositivo de seguridad portátil 109-C, por ejemplo, una tarjeta inteligente, conectada al mismo, a uno o más ordenadores servidores remotos. Estos ordenadores servidores remotos incluyen un ordenador servidor 115-C de un proveedor de servicios 115-E, un ordenador servidor 117-C de un servicio separador 117-E, un ordenador servidor 119-C de una entidad proveedora de identidad 119-E. El ordenador anfitrión 103-C es operado por un usuario 101 que interactúa con los servicios que se ejecutan en uno o más de los ordenadores servidores a través de una ventana de navegador web 105 de un navegador web 103-S que se ejecuta en el ordenador anfitrión 103.

La Figura 2 es una ilustración esquemática de programas de software correspondientes a los nodos de hardware de la Figura 1. Como se señaló anteriormente, el usuario 101 interactúa con un servicio web 115-S que se ejecuta en el ordenador servidor de proveedor de servicios 115-C. El papel del separador 117-S que se ejecuta en el servidor separador de cómputo 117-C y el proveedor de identidad 119-S que se ejecuta en el ordenador proveedor de identidad 119-C se describen a continuación.

En el escenario de ejemplo ilustrado en la Figura 1, la tarjeta inteligente 109 proporciona las operaciones criptográficas en nombre del usuario 101, por ejemplo, para firmar documentos criptográficamente, descifrar mensajes o realizar una operación criptográfica como parte de un mecanismo de autenticación de desafío-respuesta. La tarjeta inteligente también ejecuta un programa de agente de tarjeta 109-S que proporciona parte de una funcionalidad a la que se hace referencia en el presente documento como agente de usuario.

Cada uno de los ordenadores 103-C, 115-C, 117-C y 119-C puede tener componentes típicos de un ordenador, por ejemplo, una unidad de procesamiento central capaz de ejecutar instrucciones almacenadas en un dispositivo de almacenamiento y memoria utilizada durante la ejecución de programas. Los detalles de tales arquitecturas son generalmente conocidos y no son necesarios para la comprensión de la presente discusión. En un escenario, los ordenadores n-C tienen sus respectivos programas de software n-S almacenados en un dispositivo de almacenamiento del ordenador n-C. Un sistema operativo del ordenador n-C carga el programa de software n-S para ser ejecutado por el procesador del ordenador n-C. En este documento, un lenguaje como "el navegador web 103 envía un mensaje X al proveedor de servicios 115" se usa como una descripción abreviada de las acciones realizadas por los diversos procesadores que ejecutan las instrucciones de programa. Por lo tanto, la frase de ejemplo en la oración anterior podría interpretarse en el sentido de que las instrucciones de software del navegador web 103-S se ejecutan para hacer que el procesador del ordenador anfitrión 103-C transmita el mensaje X al ordenador servidor de proveedor de servicios 115-C que opera bajo las instrucciones del programa de servicio web 115-S.

La Figura 3 es una ilustración esquemática de un dispositivo de seguridad 109, por ejemplo, una tarjeta inteligente. El dispositivo de seguridad portátil 109 puede incluir un procesador 201 conectado a través de un bus 202 a una memoria de acceso aleatorio (RAM) 203, una memoria de solo lectura (ROM) 204 y una memoria no volátil (NVM) 205. El dispositivo de seguridad portátil 109 incluye además una interfaz de entrada/salida 207 para conectar el procesador 201, de nuevo típicamente a través del bus 202, a un conector 211 mediante el que el dispositivo de seguridad portátil 109 puede conectarse al ordenador anfitrión 103.

En realizaciones alternativas, la conexión entre el ordenador anfitrión 103 y el dispositivo de seguridad portátil 109 es inalámbrica, por ejemplo, utilizando comunicación de campo cercano (NFC) u otras tecnologías de comunicación por radio o microondas.

La NVM 205 y/o la ROM 204 pueden incluir programas de ordenador 301 como se ilustra en la Figura 4. Si bien aquí se representa que los programas de ordenador 301 están todos coubicados en la ROM 204 o la NVM 205, en la práctica real no existe tal restricción, ya que los programas pueden extenderse sobre múltiples memorias e incluso

instalarse temporalmente en la RAM 203. Además, el dispositivo de seguridad portátil 109 puede incluir múltiples ROM o NVM. Los programas 301 incluyen programas del sistema operativo así como programas de aplicación cargados en el dispositivo de seguridad portátil 109. La NVM 205 o la ROM 204 también pueden contener datos privados, tales como una clave privada 209 o una clave secreta compartida 210, almacenada en su forma básica o en cantidades derivadas.

Los programas 301 del dispositivo de seguridad portátil 109 pueden incluir un módulo de criptografía 213, un módulo de autenticación de usuario 215, un módulo de comunicaciones 217 y el sistema operativo SO 219. Los programas 301 del dispositivo de seguridad portátil 109 pueden incluir además un agente de tarjeta 221 para hacer que el dispositivo de seguridad portátil 109 realice las tareas del dispositivo de seguridad portátil 109 descrito aquí, por ejemplo, negociar un protocolo de emisión de credenciales para generar una credencial preservadora de privacidad.

De acuerdo con la Guía de autenticación electrónica del NIST, una credencial es "un objeto o estructura de datos que vincula de manera autorizada una identidad (y opcionalmente, atributos adicionales) a un token poseído y controlado por un suscriptor" NIST "Electronic Authentication Guideline", Publicación especial del NIST 800-63-1 (Borrador 3), junio de 2011. Una autoridad, por ejemplo, el proveedor de identidad (IdP) 119, emite una credencial a un usuario 101. Entre los ejemplos de credenciales se incluyen el nombre de usuario y la contraseña o un certificado X.509 y su clave privada correspondiente.

Una credencial anónima permite al usuario demostrarle a un proveedor de servicios (SP) que la credencial contiene los atributos requeridos sin revelar la información almacenada dentro de la credencial. Por ejemplo, el usuario puede demostrar que es mayor de 18 años sin revelar su fecha de nacimiento. La credencial anónima, por lo tanto, prueba el atributo en cuestión y al mismo tiempo protege la privacidad del usuario. Una tecnología de credenciales anónimas permite construir un sistema de identidad de mejora de privacidad y que separa la emisión de credenciales y el uso de credenciales.

El proveedor de identidad (IdP) 119 es el emisor de credenciales. Los usuarios 101 y los proveedores de servicios 115 confían en él. El IdP 119 conoce o puede conocer información de identidad de los usuarios y puede verificar la información. Aunque alguna tecnología de credenciales anónimas, como Idemix, permite a los usuarios ocultar ciertos atributos del IdP 119, el IdP 119 aún conoce cierta información de identidad sobre el usuario y, por lo tanto, puede responder por la información. En un sistema de identidad de mejora de privacidad, el IdP 119 no conoce el identificador de una credencial que ha emitido. El usuario, que opera el ordenador anfitrión 103 y el dispositivo de seguridad 109, crea el identificador. Este proceso garantiza que no se pueda rastrear el identificador.

Poder ocultar atributos del IdP 119 es útil tanto para credenciales específicas de dominio como si el usuario desea elegir un seudónimo sin revelarlo a los emisores de credenciales. De lo contrario, el emisor de credenciales y el IdP pueden coludirse para rastrear seudónimos y obtener la(s) identidad(es) relacionada(s) con ese seudónimo.

La Figura 5 es un diagrama de bloques que ilustra la emisión y el uso de una credencial preservadora de privacidad. El proveedor de identidad 119 emite la credencial 503, etapa 501. El usuario 101 almacena la credencial 503. Esta puede estar en el ordenador anfitrión 103 del usuario o en el dispositivo de seguridad 109. El usuario produce un token de presentación 507 a partir de la credencial 503 y lo presenta al proveedor de servicios 115. El proveedor de servicios 115 verifica los tokens de presentación que se le presentan, etapa 509, y proporciona servicios web 511.

El proveedor de identidad (IdP) 119 emite credenciales a los usuarios finales 101. La emisión de credenciales es un proceso interactivo entre el IdP 119 y el usuario 101 (a través del agente de usuario). El agente de usuario puede ser una combinación de software conocido como agente de tarjeta 221 y software que se ejecuta en el ordenador anfitrión 103, por ejemplo, dentro del navegador web 103-S. Al final del protocolo, el dispositivo de seguridad del usuario (por ejemplo, tarjeta inteligente) 109 tiene el token de credencial 503 y lo almacena en la memoria segura del dispositivo.

El proveedor de servicios (SP) 115 verifica la credencial del usuario antes de proporcionar los servicios solicitados 511. Para un ecosistema de identidad de mejora de privacidad, el usuario 101 no proporciona su credencial al SP directamente. En cambio, el SP especifica su política de control de acceso y el usuario demuestra que cumple los requisitos de la política sin presentar la credencial directamente. Para este propósito, el usuario presenta un token de presentación 509 que el SP 115 puede verificar 509.

El usuario, a través de su dispositivo de seguridad 109, genera un token de presentación 507 a partir de la credencial 503 basándose en la política del SP 115 y presenta el token al SP. El token de presentación podría ser, por ejemplo, una prueba de presentación de UProve, una prueba de Idemix o una credencial firmada basada en mERA.

El SP 115 verifica el token de presentación 507, etapa 509. El SP 115 también puede necesitar verificar si la credencial 503 es nueva (en el caso de una credencial de un solo uso) o si el número de usos permitidos no se ha excedido (en el caso de una credencial de usos múltiples). La solución varía dependiendo de si la credencial 503 es específica de SP o no.

El usuario 101 interactúa con entidades a través de internet a través del agente de usuario que puede incluir el navegador web 103-C del usuario, la tarjeta inteligente 109 y otro hardware o software que actúan en nombre del usuario. El usuario (a través de un agente de usuario) obtiene una credencial 503 del IdP 119 y usa la credencial 503

en varios SP en forma de tokens de presentación 507 creados basándose en las políticas particulares de los SP 115.

El dispositivo de seguridad 109 del usuario obtiene la credencial 503 del IdP 119 usando un protocolo de emisión de credenciales. Al final del protocolo, el dispositivo de seguridad 109 genera u obtiene la credencial 503.

El usuario 101 usa la credencial cuando interactúa con un SP 115. La tarjeta inteligente 109 genera un token de presentación 507 a partir de la credencial 503 basándose en los requisitos del SP 115.

Hay dos tipos de flujos de interacción en términos de emisión y uso de tokens de credenciales: previa a emisión y emisión bajo demanda.

En un flujo previo a emisión, el usuario 101 primero inicia la obtención del token de credencial del IdP 119, después de lo cual el usuario 101 usa el token con el proveedor de servicios 115. Este flujo separa completamente la emisión de token y el uso de token y, por lo tanto, preserva las características de privacidad ofrecidas por la criptografía subyacente. Este proceso se aproxima mejor a los patrones de papeleo típicos y más familiares del mundo físico donde un usuario obtiene una credencial, como una licencia de conducir o una tarjeta de seguro médico de una autoridad otorgante, y luego la credencial se usa cuando es necesario después de haber sido otorgada. Sin embargo, el mundo en línea actual a menudo opera en el modo de obtener una credencial de identidad solo en el momento en que se necesita.

En el flujo bajo demanda, el usuario 101 comienza visitando un servicio web de proveedor de servicios (SP) 115 que solicita al usuario 101 que presente una determinada credencial. En el escenario de flujo bajo demanda, ni el usuario 101 ni el dispositivo de seguridad 109 del usuario ya tienen la credencial requerida para satisfacer los requisitos del SP 115. El SP 115 indica al usuario que obtenga la credencial dinámicamente de un IdP 119, que puede ser determinado por el SP 115 o por el usuario 101 dependiendo de las circunstancias. El usuario 101 que acepta obtener la credencial 503 del IdP 119 - haciendo clic en un enlace, por ejemplo - puede ser considerado como consentimiento del usuario. Sin embargo, algunos casos de uso pueden requerir un consentimiento más explícito del usuario. Después de obtener el token de credencial, el usuario regresa al SP 115 para presentar el token como token de presentación 507.

Una vez que el usuario 101 obtiene la credencial 503, el usuario 101 puede reutilizar la credencial 503 y también podría usar la credencial 503 con SP 115 diferentes y no relacionados. Por lo tanto, después de obtener el token, el uso de la credencial 503 se convierte en el mismo proceso que el caso de flujo previo a emisión.

La Figura 6 es un diagrama de secuencia temporal que ilustra el flujo de datos en un escenario previo a emisión. En el flujo previo a emisión, la emisión de token (credencial) y el uso de token están separados. El token se puede utilizar con varios SP sin que los SP se registren con la tarjeta. La tarjeta tiene uno o varios tokens, que incluyen varios atributos. El titular de la tarjeta decide qué revelar al SP. En este caso, el usuario va al IdP 119 para obtener un token. Luego va a varios SP y usa el token.

El usuario se acerca al IdP 119 para obtener una credencial y participa en un intercambio de autenticación de usuario, etapa 601. La autenticación de usuario puede implicar al dispositivo de seguridad 109 del usuario. A continuación, el dispositivo de seguridad 109 y el IdP 119 participa en un Protocolo de Emisión de Token, etapa 603. Un ejemplo de un protocolo de emisión de tokens es el protocolo de emisión de tokens de U-Prove que se describe en Christian Paquin, "U-Prove cryptographic specifics", v1.1, Microsoft Corporation, febrero de 2011. http://connect.microsoft.com/site1188/Downloads/DownloadDetails.aspx?DownloadID=33 918, consultado el 16 de diciembre de 2012. Tras la conclusión del intercambio de protocolo de emisión de token 603, el dispositivo de seguridad 109 genera el token de credencial, etapa 605, después de lo cual el agente de usuario, en este caso el dispositivo de seguridad 109, comunica un mensaje de estado 607 al IdP 119 indicando que el token de credencial ha sido creado. Los intercambios entre el dispositivo de seguridad 109 y el IdP 119 pueden ocurrir a través del navegador web 103 como se indica por los puntos circulares sólidos en la Figura 6.

La Figura 7 es un diagrama de secuencia temporal que ilustra el uso de una credencial y un token de presentación generada a partir de la misma. El usuario 101 comienza visitando un servicio web 115, etapa 701. El servicio web 115 responde al navegador con una solicitud de un token de presentación que satisface una política especificada, etapa 703.

El navegador 103 reenvía esta solicitud de token al dispositivo de seguridad 109, etapa 705. El dispositivo de seguridad genera la prueba requerida, etapa 707, en forma de token de presentación 507, y envía el token de presentación al servicio web 115, etapa 709.

El servicio web 115 verifica el token de presentación, etapa 711, y si todo está bien con respecto al mismo, es decir, el token de presentación satisface la política de autorización del servicio web 115, el servicio web otorga el acceso solicitado, etapa 713.

El flujo bajo demanda es similar al inicio de sesión único web (SSO). Con el flujo bajo demanda, es muy difícil, si no imposible, separar completamente la emisión de token y el uso de token porque la correlación de tiempo siempre es posible. Por lo tanto, la imposibilidad de rastrear es difícil de lograr.

Hay más de una forma de diseñar el flujo de emisión bajo demanda. Cada uno tiene sus ventajas y desventajas. En el flujo bajo demanda es deseable separar el emisor de credenciales (IdP) 119 del proveedor de servicios (SP) 115. Una forma de lograrlo es utilizar un agente remoto 117, denominado en el presente documento como separador 117. El separador 117 se describe con mayor detalle a continuación. Este método permite la emisión bajo demanda de credenciales preservadoras de privacidad, separa a los proveedores de servicios del emisor de credenciales (por ejemplo, el proveedor de identidad IdP 119) y logra objetivos de privacidad al tiempo que brinda una experiencia de usuario sin interrupciones. Los componentes principales del proceso son el dispositivo seguro 109 (por ejemplo, una tarjeta inteligente), el separador 117 y la realización de una doble redirección de solicitudes de credenciales o solicitudes de token de presentación.

1. El dispositivo de seguridad 109 conserva las claves privadas del usuario, genera y almacena la credencial de usuario (token) y calcula las pruebas de presentación (token de presentación).

2. El separador 117 está alojado por un tercero de confianza (servicio de separador 117-E) que separa el SP 115 del IdP 119 para que el IdP 119 no sepa con qué SP 115 ha interactuado el usuario 101 o cuándo tuvo lugar dicha interacción. El separador 117 conoce el SP 115 y el IdP 119. Sin embargo, el separador 117 no sabe quién es el usuario 101 y no conoce la credencial 503 del usuario.

3. La doble redirección del flujo de mensajes es el mecanismo de la separación.

La Figura 8 es un diagrama de secuencia temporal que ilustra un método que implica redirecciones dobles de una solicitud de token del proveedor de servicios a través de un separador. Por motivos de seguridad, todas las comunicaciones a través de internet deben utilizar un protocolo seguro, por ejemplo, SSL / TLS.

Etapa 801: Un usuario 101 visita el servicio web 115 del SP a través de un navegador web 103.

Etapa 803: El SP 115 solicita ciertos atributos de la credencial de un usuario (denominada token de presentación) al especificar una política (también denominada criterios). Esto presenta dos escenarios posibles: primero, el caso trivial en el que el usuario tiene una credencial 503 y por lo tanto ya tiene la capacidad de generar la prueba requerida y presentarla en un token de presentación, y, segundo, donde el usuario no tiene la credencial 503 y debe procurar una. La discusión subsiguiente del proceso restante de la Figura 8 que sigue aquí describe el flujo para el segundo caso.

La interacción entre el usuario 101 y el servicio web del SP 115 a través del navegador 103 se representa en la Figura 9a. El SP 115 muestra un texto 901 pidiendo al usuario 101 que inicie sesión y proporciona un botón 903 para presionar cuando esté listo. Si el usuario tiene una credencial 503, se genera el token de presentación requerido y puede continuar el procedimiento de inicio de sesión. Ese escenario, al ser un caso trivial, no se presenta en la Figura 8.

Cabe señalar que la interacción del usuario a través de las pantallas de interfaz de usuario 9a a 9d son simplemente un ejemplo de un posible flujo. Por ejemplo, en otras alternativas, el flujo puede estar más automatizado.

En el escenario ilustrado, el dispositivo de seguridad 109, que puede ser una tarjeta inteligente, no tiene la credencial (token) y responde con un mensaje 805 a tal efecto. Esto hace que el SP 115 produzca una indicación de que debe generarse una credencial 503 junto con un proveedor de identidad 119. Un ejemplo de esto se ilustra en la Figura 9b. Se muestra un texto de información 905 y se proporciona un botón 907 para que el usuario continúe. Alternativamente, estas etapas ocurren automáticamente sin interacción directa con el usuario. En otra alternativa más, el SP 115 informa al usuario que obtenga una credencial del proveedor de identidad 119.

Etapa 807: El SP 115 indica al usuario que obtenga la credencial dinámicamente enviando un mensaje para hacerlo al navegador 103, por ejemplo, como se muestra en la Figura 9b. Esta tarea se lleva a cabo mediante una redirección (etapa 809) desde el SP 115 al separador 117 y una segunda redirección (etapa 815) desde el separador 117 al IdP 119.

Etapa 807: Dado que el dispositivo de seguridad 109 respondió con una respuesta "No Token" en la etapa 805, el SP 115 muestra un texto 907 que le dice al usuario que obtenga una credencial 503 a través del proveedor de identidad 119 y proporciona el botón 907 para hacer clic. Cuando el usuario hace clic en el botón, el SP 115 envía un mensaje, que incluye un enlace al separador 117, al navegador 103 solicitando la generación de credenciales.

Etapa 809: El navegador 103 redirige la solicitud de generación de credenciales enviando la solicitud al separador 117, etapa 811. Cuando el separador 117 recibe la solicitud 811 del navegador 103, el separador 117 responde con una dirección al control de transferencia del navegador 103 al proveedor de identidad 119. Desde la perspectiva del proveedor de identidad 119, la solicitud se originó desde el separador 117.

Por lo tanto, el flujo de emisión de credenciales bajo demanda requiere redirecciones entre tres partes, aquí identificadas como SP 115, separador 117 e IdP 119. Para este propósito pueden usarse protocolos estándar existentes, como SAML 2.0 o WS_ *, sin embargo, los protocolos estándar no proporcionan las características de preservación de privacidad deseadas en un sistema de privacidad. En una realización preferida, la redirección a través del separador 117 funciona para proteger mejor la privacidad del usuario. Se debe utilizar HTTPS para garantizar la confidencialidad y la integridad de las comunicaciones entre los diferentes nodos de internet.

Etapa 813: El separador 117 envía la solicitud sin la característica de identificación de fuente de vuelta al navegador 103 para una segunda redirección, etapa 815, esta vez al IdP 119, etapa 817. La Figura 9c ilustra un ejemplo de página de destino en el proveedor de identidad 119 con un texto de invitación 907 al usuario 101 para generar una credencial y un botón 911 para hacer clic para iniciar ese proceso.

Etapa 819: El IdP 119 autentica al usuario 101, por ejemplo, a través del dispositivo de seguridad a través del navegador 103.

Etapa 821: El IdP 119 y el dispositivo de seguridad 109 ejecutan el protocolo de emisión de tokens. El protocolo de emisión es un intercambio entre el IdP 119 y el dispositivo de seguridad 109. El IdP 119 verifica y da fe de la validez de los atributos que el usuario 101 puede necesitar probar posteriormente. El IdP 119 ya conoce, a través del intercambio de protocolo de emisión, los valores de atributo seleccionados ya que el IdP 119 debe estar equipado para dar fe de su veracidad. Sin embargo, el IdP 119 nunca se da cuenta del identificador de token que el dispositivo de seguridad 109 asocia con la credencial 503, también denominado token.

Etapa 823: El dispositivo de seguridad 109 genera y almacena la credencial 503 (por ejemplo, token U-Prove, credencial idemix) y devuelve un mensaje de estado, etapa 825, al IdP que indica la finalización de la generación de la credencial 503.

En las etapas 827 - 835, el IdP 119 transmite el estado de emisión de token al SP 115, nuevamente a través del proceso de redireccionamiento doble como se describe anteriormente pero en orden inverso, utilizando el separador 117. Primero, desde el IdP 119 al separador 117 a través del navegador 103, etapas 827, 829 y 831, y luego desde el separador 117 al SP 115 a través del navegador 103, etapas 833, 835 y 837.

Etapa 839: En caso de que el estado sea correcto, es decir, el SP 115 recibe correctamente el mensaje emitido por token e indica al SP 115 que se ha generado correctamente una credencial válida, el SP 115 repite la solicitud de un token de presentación 507 del usuario 101. La solicitud es recibida por el navegador 103 y manejada por el dispositivo de seguridad 109. La Figura 9d ilustra la interacción con el usuario 101 del proveedor de servicios para crear el token de presentación. El proveedor de servicios 115 presenta un botón 915 que solicita al usuario que presente el token de presentación. Al hacer clic en el botón 915, se envía el mensaje 840 al dispositivo de seguridad 109 solicitando al dispositivo de seguridad 109 para que genere el token de presentación de acuerdo con la política del proveedor de servicios 109.

En la etapa 841, el dispositivo de seguridad 109 genera la prueba (token de presentación 507). En el caso de U-Prove, la prueba se conoce como prueba de presentación o, en el caso de idemix, una transformación de la credencial idemix en una credencial que solo contiene el subconjunto de la información en la credencial que el usuario debe dar fe.

En la etapa 843, el dispositivo de seguridad 109 envía el token de presentación 507 al SP 115. Por ejemplo, en el caso de U-Prove, el navegador y el SP 115 ejecutan un protocolo de presentación, que incluye probar atributos que son parte de la política del SP e incluye la firma del proveedor de identidad, una clave pública específica de token del token y una respuesta a un desafío de presentación del SP 115.

En la etapa 845, el SP 115 verifica el token de presentación 507. Si el token de presentación es satisfactorio, el SP 115 proporciona los servicios solicitados al usuario, Etapa 847.

Para que funcionen las operaciones de redireccionamiento, el separador 117 debe poder asociar solicitudes de token con los SP 115 apropiados. Una forma sencilla es que el separador 117 mantenga un mapa de solicitudes y SP. Este enfoque puede ser vulnerable a ataques de denegación de servicio. Alternativamente, el separador 117 puede codificar la información de identificación del SP 115 en la solicitud al IdP 119 de tal manera que solo el separador 117 puede recuperar la información, por ejemplo, mediante encriptación. Otra alternativa es que el separador 117 escriba una cookie en el ordenador 103 del usuario y lea la cookie más tarde cuando el separador necesite conocer el SP de origen 115.

El flujo de alto nivel en la Figura 8 se aplica a varias tecnologías de mejora de privacidad como U-Prove, idemix u otras, aunque estas tecnologías difieren en su criptografía subyacente, protocolo de emisión, protocolo de presentación, especificación de políticas y formato de token.

Con respecto al flujo bajo demanda, la vinculación de la emisión de token y el primer uso del token es potencialmente posible, si el IdP 119, el SP 115 y el separador 117 (tercero confiable) todos coluden y hacen una correlación de tiempo. Sin embargo, la introducción del separador 117 hace mucho más difícil coludir debido a la existencia del tercero. Además, la vinculación es mucho más difícil que el enfoque de agente de usuario de Microsoft, donde el agente de usuario conoce mucha información sobre la transacción, por ejemplo, qué usuario, qué IdP, qué SP, qué credenciales y en qué momento. El separador 117 no sabe nada sobre los usuarios o sus credenciales, y sirve solo como un conducto opaco para el proceso.

A partir de lo anterior, será evidente que se ha presentado una tecnología que proporciona un método conveniente para el uso práctico de credenciales preservadoras de privacidad en el entorno de internet, con el que los usuarios pueden obtener dinámicamente las credenciales preservadoras de privacidad cuando sea necesario sin perder la

conveniencia y la privacidad.

Aunque se han descrito e ilustrado realizaciones específicas de la invención, la invención no debe limitarse a las formas o disposiciones específicas de las partes así descritas e ilustradas.

REIVINDICACIONES

1. Un método para autenticar a un usuario, que opera una aplicación web en un ordenador anfitrión, en un servicio basado en web de un proveedor de servicios (115), en donde el método comprende:

- redireccionar una solicitud para generar una credencial desde el proveedor de servicios (115) a un proveedor de identidad (119) a través de un separador (117) ejecutado en un ordenador servidor separador (117-C) y operado por un tercero de confianza, al:

transmitir una primera solicitud (807, 809, 811) de una credencial al separador (117);

operar el separador (117) para devolver una segunda solicitud (813, 815, 817) de la credencial a la aplicación web, esta segunda solicitud redirige la aplicación web a un proveedor de identidad (119) de modo que desde la perspectiva del proveedor de identidad (119), la segunda solicitud se origina desde el separador (117);

- operar el proveedor de identidad (119) y un dispositivo de seguridad (109) asociado con el usuario y conectado al ordenador anfitrión:

para participar en un intercambio de creación de credenciales preservadoras de privacidad (819, 821, 823, 825, 827, 829, 831, 833, 835, 837) a través de la aplicación web y en cooperación con el proveedor de identidad (119);

- operar el dispositivo de seguridad (109) para generar (839, 840, 841) un token de presentación a partir de la credencial preservadora de privacidad; y

presentar (843) a través de la aplicación web el token de presentación al proveedor de servicios como prueba de un atributo.

2. El método para autenticar a un usuario según la reivindicación 1

- en donde la solicitud para generar una credencial está precedida por operar el proveedor de servicios (115) para solicitar una prueba de un atributo del usuario;

- y el método comprende además:

transmitir un mensaje de estado emitido por token desde el proveedor de identidad (119) a la aplicación web (115);

operar el ordenador anfitrión para redirigir el mensaje de estado emitido por token al separador (117);

operar el separador (117) para redirigir el mensaje de estado emitido por token al proveedor de servicios (115) a través del ordenador anfitrión; y

- en donde la etapa de operar el dispositivo de seguridad (109) para crear un token de presentación a partir de la credencial preservadora de privacidad es precedido por operar el proveedor de servicios, en respuesta a la recepción del mensaje de estado emitido por token, para repetir la solicitud de prueba de un atributo del usuario.

3. El método para autenticar a un usuario según la reivindicación 2, en donde además comprende:

operar el proveedor de servicios (115) para verificar el token de presentación y proporcionar acceso al servicio del proveedor de servicios.

4. El método para autenticar a un usuario según la reivindicación 1, en donde comprende además operar el dispositivo de seguridad (109) para almacenar la credencial preservadora de privacidad o el token de presentación.

5. El método para autenticar a un usuario según la reivindicación 1, en donde el dispositivo de seguridad (109) es una tarjeta inteligente.

6. El método para autenticar a un usuario según la reivindicación 1, en donde la credencial es una credencial preservadora de privacidad de U-Prove.

7. El método para autenticar a un usuario según la reivindicación 1, en donde la credencial es una credencial idemix Identity Mixer y el token de presentación es una transformación de la credencial idemix.

8. Un sistema para autenticar a un usuario, que opera una aplicación web en un ordenador anfitrión, a un servicio basado en web de un proveedor de servicios (115), en donde el sistema comprende:

- el ordenador anfitrión que opera bajo el control de la aplicación web (103) mediante el que el usuario accede al servicio basado en web que se ejecuta en un servidor del proveedor de servicios (115);

- un dispositivo de seguridad asociado con el usuario y conectado al ordenador anfitrión y programado para generar y almacenar credenciales preservadoras de privacidad, para generar tokens de presentación a partir de las

credenciales preservadoras de privacidad en respuesta a recibir, a través de la aplicación web, una solicitud que incluye una política del servicio basado en web, y presentar a través de la aplicación web los tokens de presentación al servidor del proveedor de servicios (115) como prueba de un atributo;

- en donde el servidor del proveedor de servicios se programa para generar una solicitud de generación de credenciales que redirige a un separador (117) a través de la aplicación web que se ejecuta en el ordenador anfitrión;

- en donde el separador (117), ejecutado en un ordenador servidor separador (117-C) y operado por un tercero de confianza, comprende un servidor web que se programa para recibir una solicitud de generación de credenciales y para crear una segunda solicitud de generación de credenciales, en donde el separador devuelve la segunda solicitud de generación de credenciales a la aplicación web y en donde la segunda solicitud de generación de credenciales redirige la aplicación web a un proveedor de identidad (119) de modo que desde la perspectiva del proveedor de identidad (119), se origina la segunda solicitud de generación de credenciales del separador (117); y

- en donde el proveedor de identidad (119) comprende un servidor web operable para participar en un protocolo de generación de credenciales con el dispositivo de seguridad a través de la aplicación web.

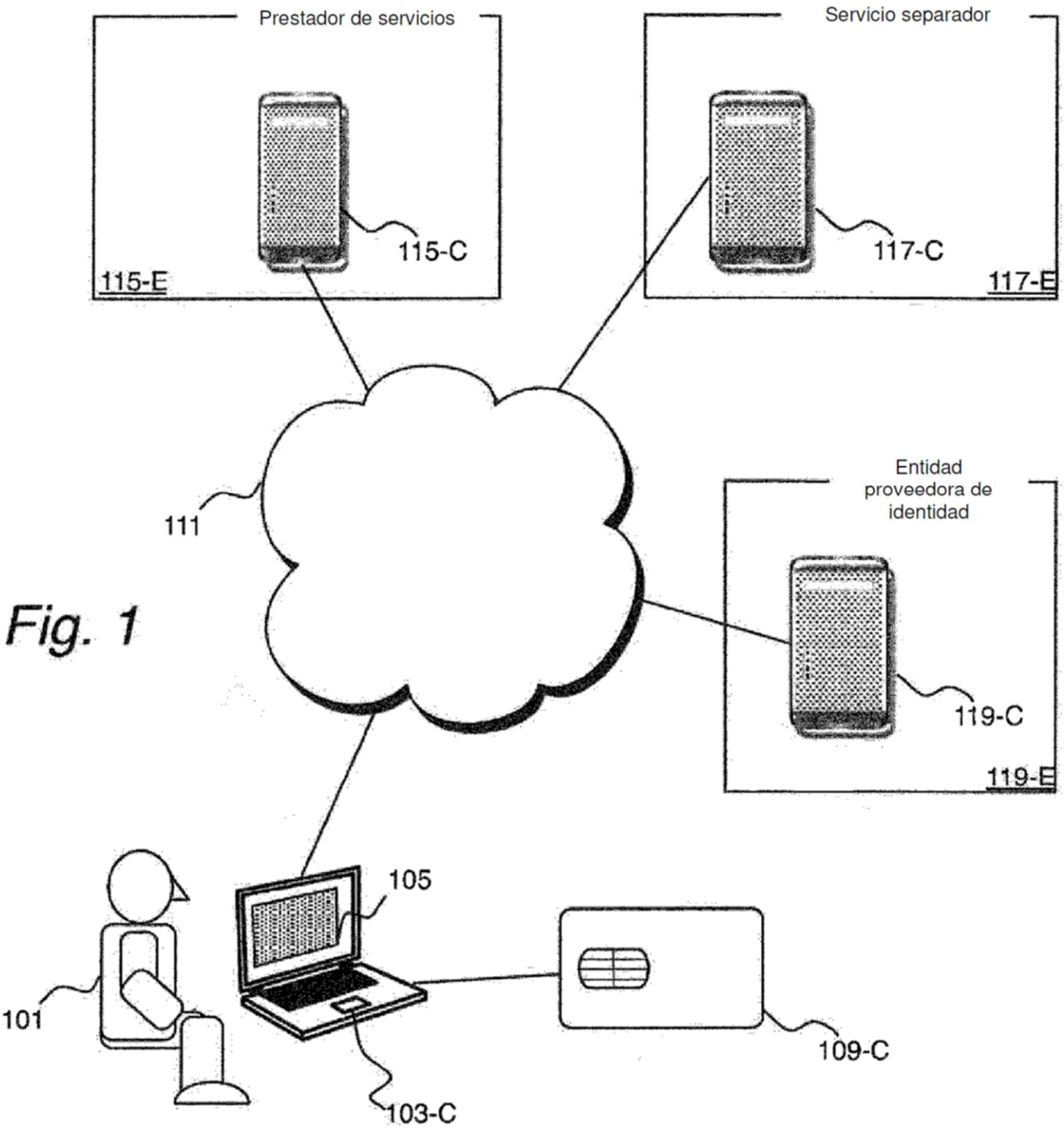
Prestador de servicios
115-C
115-E
Servicio separador
117-C
117-E
111
Entidad proveedora de identidad
119-C
119-E
105
101
109-C
103-C

Fig. 1

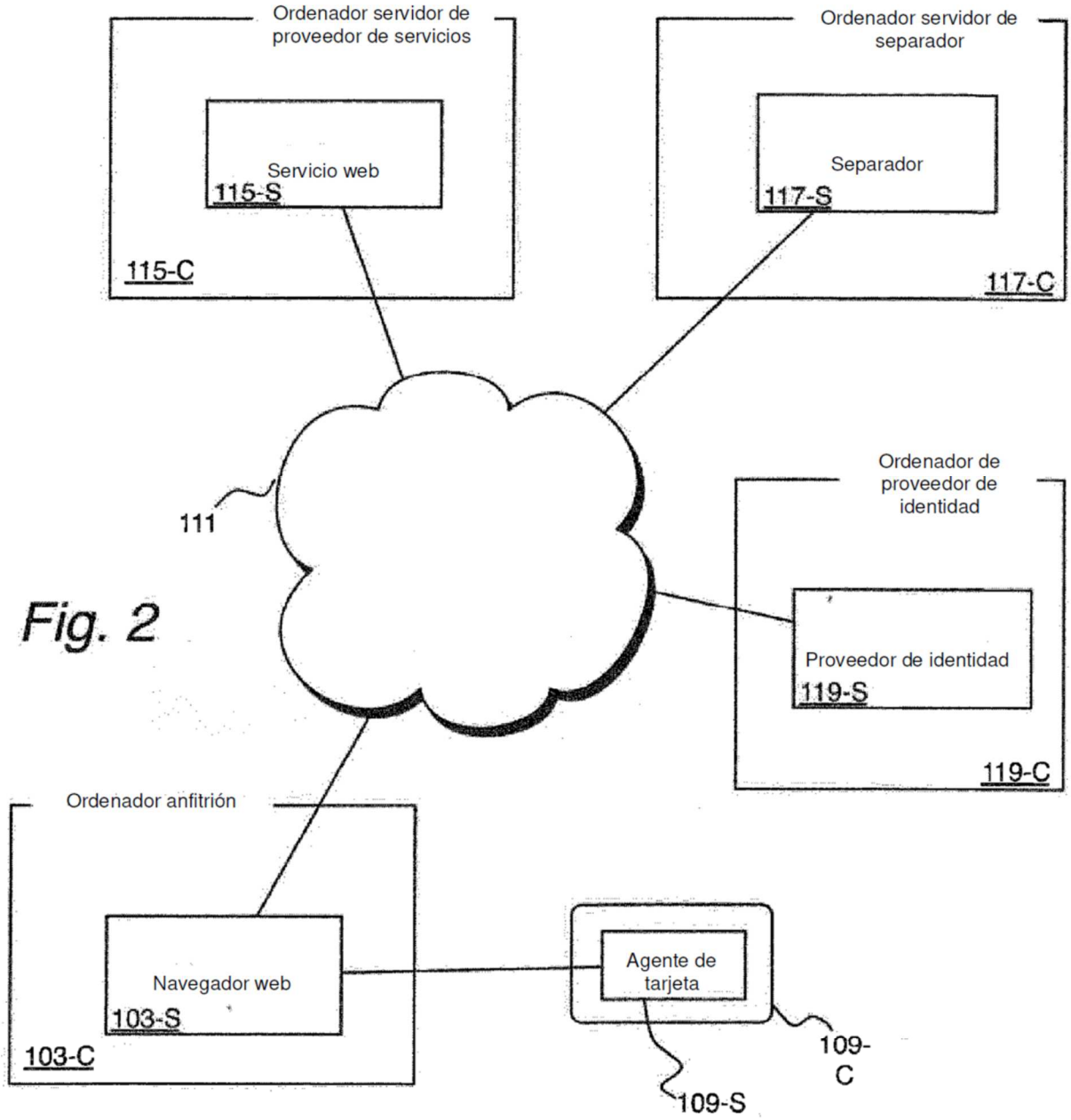
Ordenador servidor de proveedor de servicios
Servicio web
115-S
115-C
Ordenador servidor de separador
Separador
117-S
117-C
111
Ordenador de proveedor de identidad
Proveedor de identidad
119-S
119-C
Ordenador anfitrión
Navegador web
103-S
103-C
Agente de tarjeta
109-C
109-S

Fig. 2

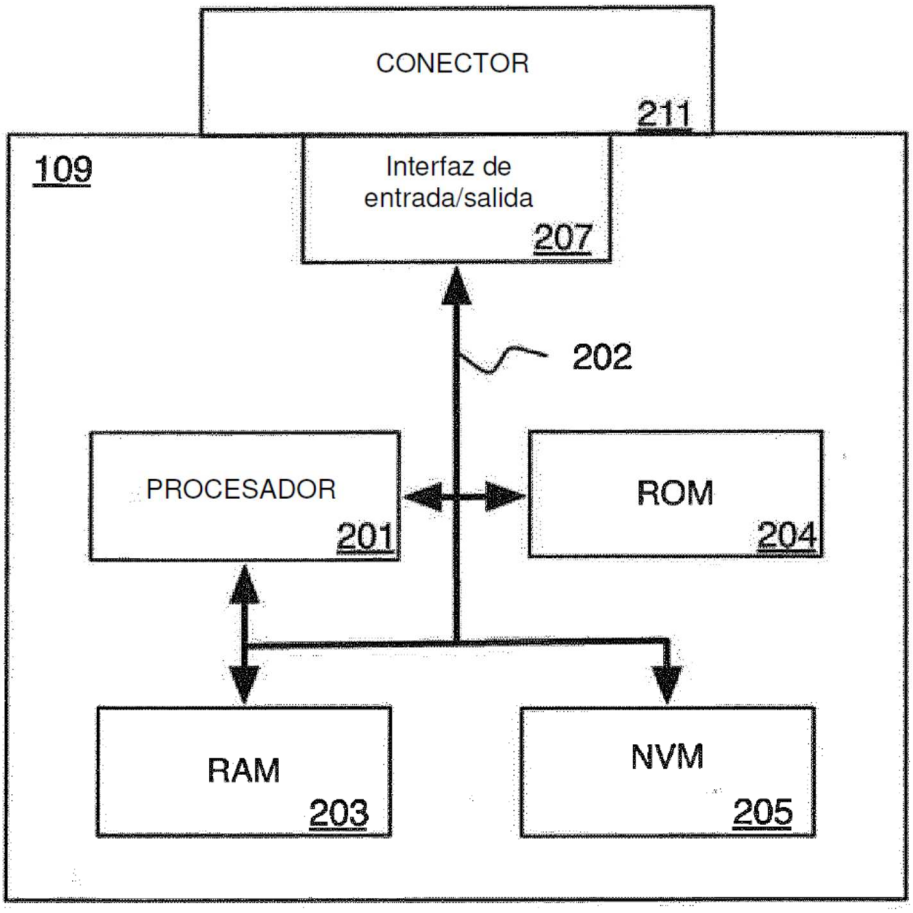
CONECTOR
211
109
Interfaz de entrada/salida
207
202
PROCESADOR
201
ROM
204
RAM
203
NVM
205

Fig. 3

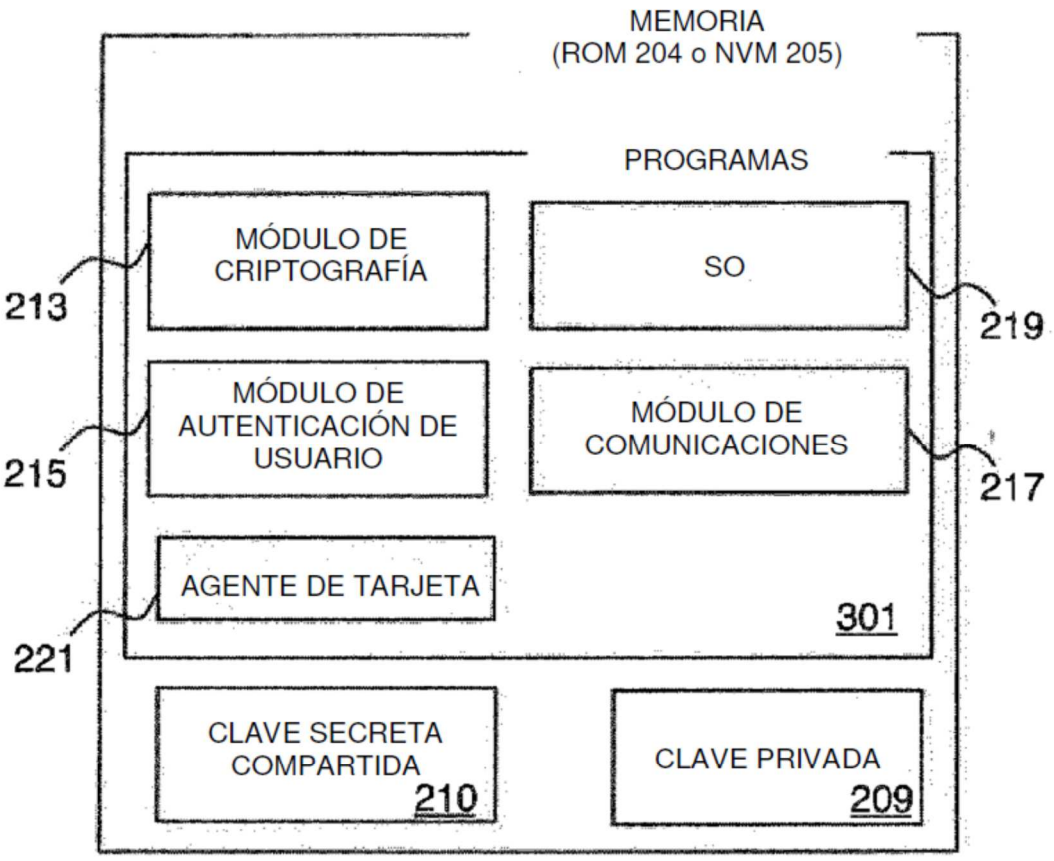
MEMORIA
(ROM 204 o NVM 205)
PROGRAMAS
MÓDULO DE CRIPTOGRAFÍA
213
SO
219
MÓDULO DE AUTENTICACIÓN DE USUARIO
215
MÓDULO DE COMUNICACIONES
217
AGENTE DE TARJETA
221
301
CLAVE SECRETA COMPARTIDA
210
CLAVE PRIVADA
209

Fig. 4

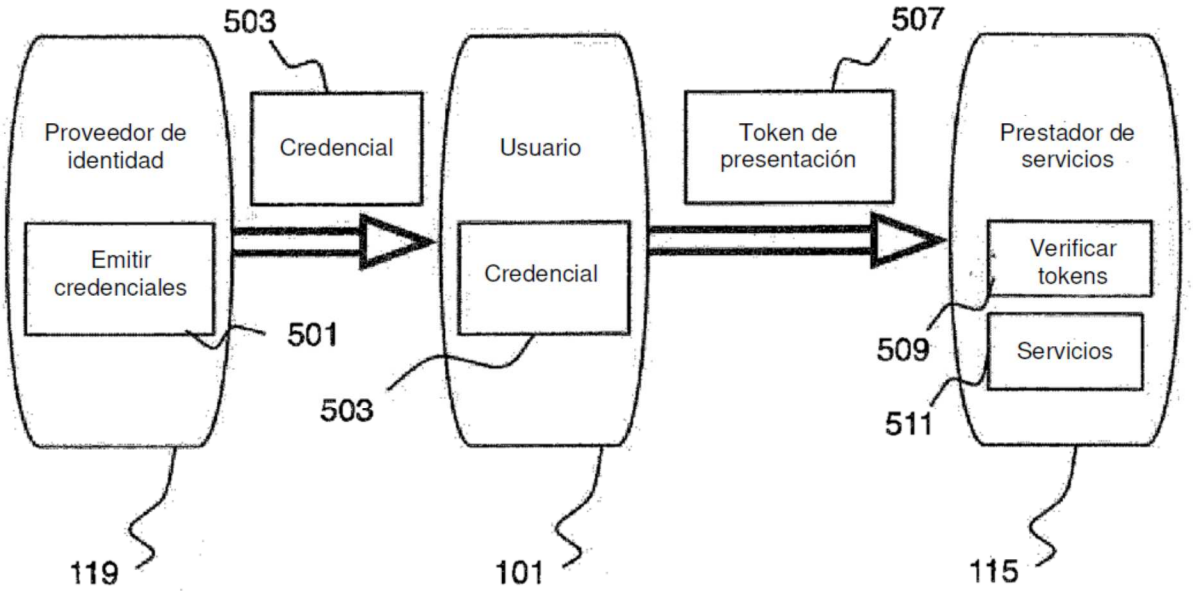
503
Proveedor de identidad
Credencial
Usuario
507
Token de presentación
Prestador de servicios
Emitir credenciales
501
Credencial
503
Verificar tokens
509
Servicios
511
119
101
115

Fig. 5

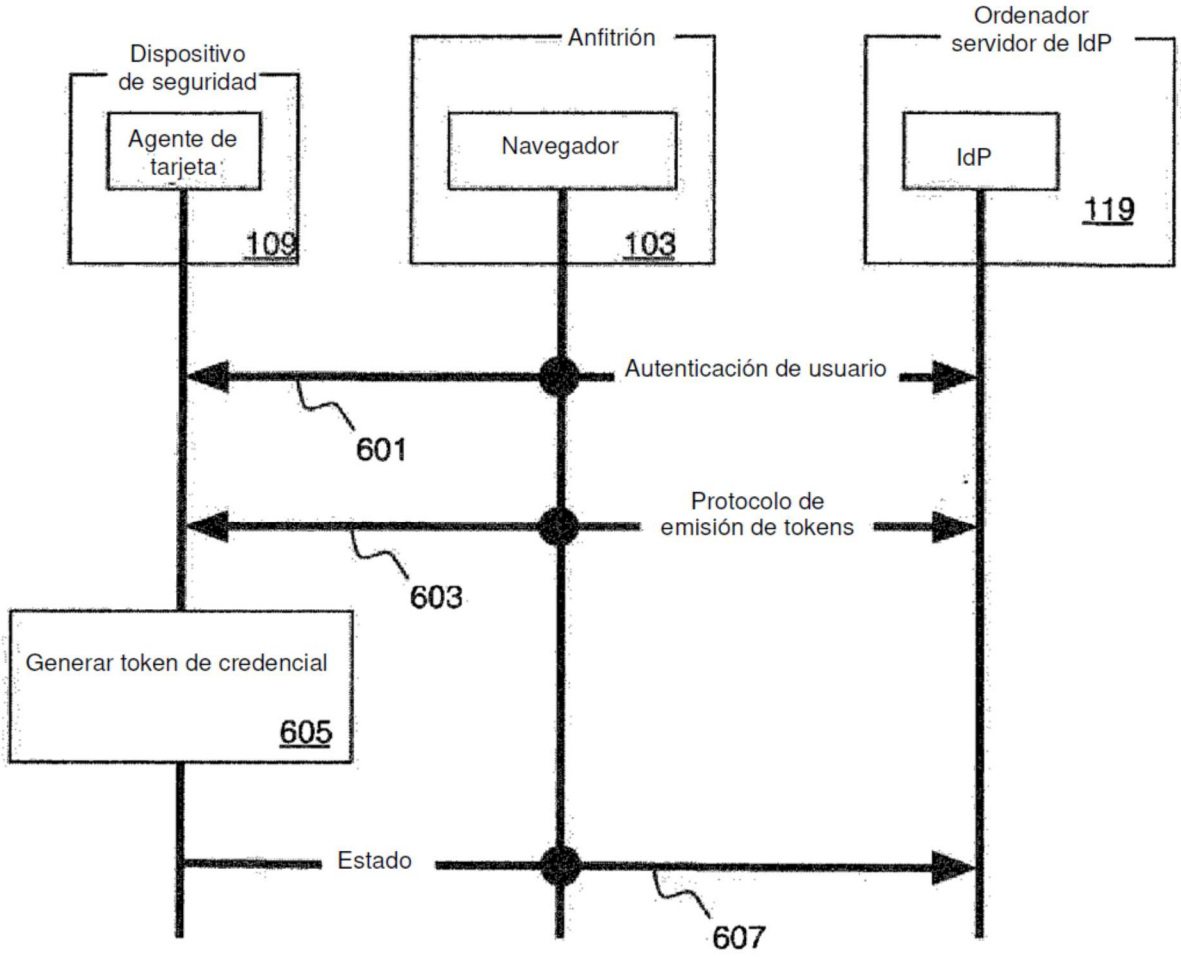
Dispositivo de seguridad
Agente de tarjeta
109
Anfitrión
Navegador
103
Ordenador servidor de IdP
IdP
119
Autenticación de usuario
601
Protocolo de emisión de tokens
603
Generar token de credencial
605
Estado
607

Fig. 6

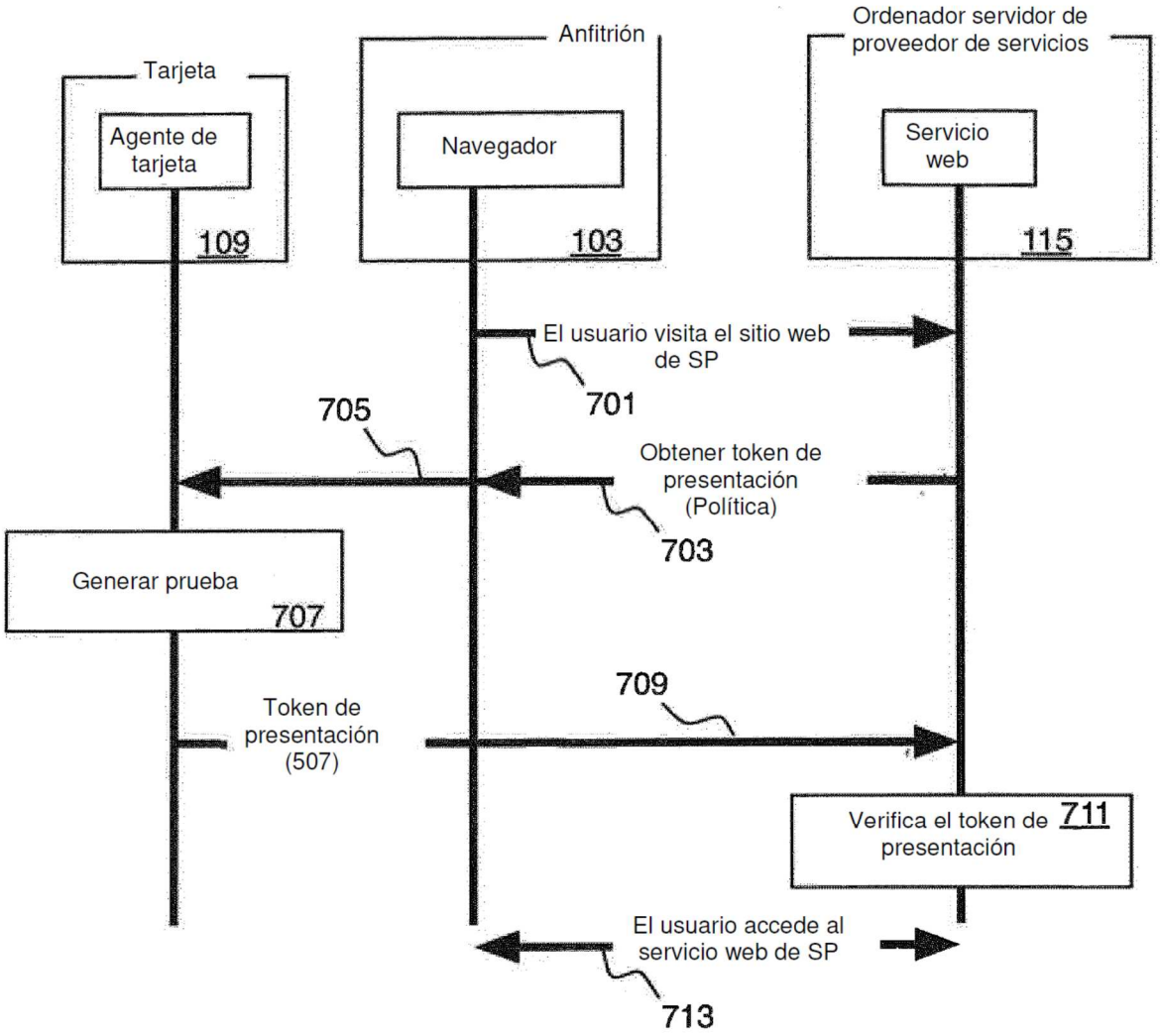
Tarjeta
Agente de tarjeta
109
Anfitrión
Navegador
103
Ordenador servidor de proveedor de servicios
Servicio web
115
El usuario visita el sitio web de SP
701
705
Obtener token de presentación (Política)
703
Generar prueba
707
709
Token de presentación (507)
Verifica el token de presentación
711
El usuario accede al servicio web de SP
713

Fig. 7

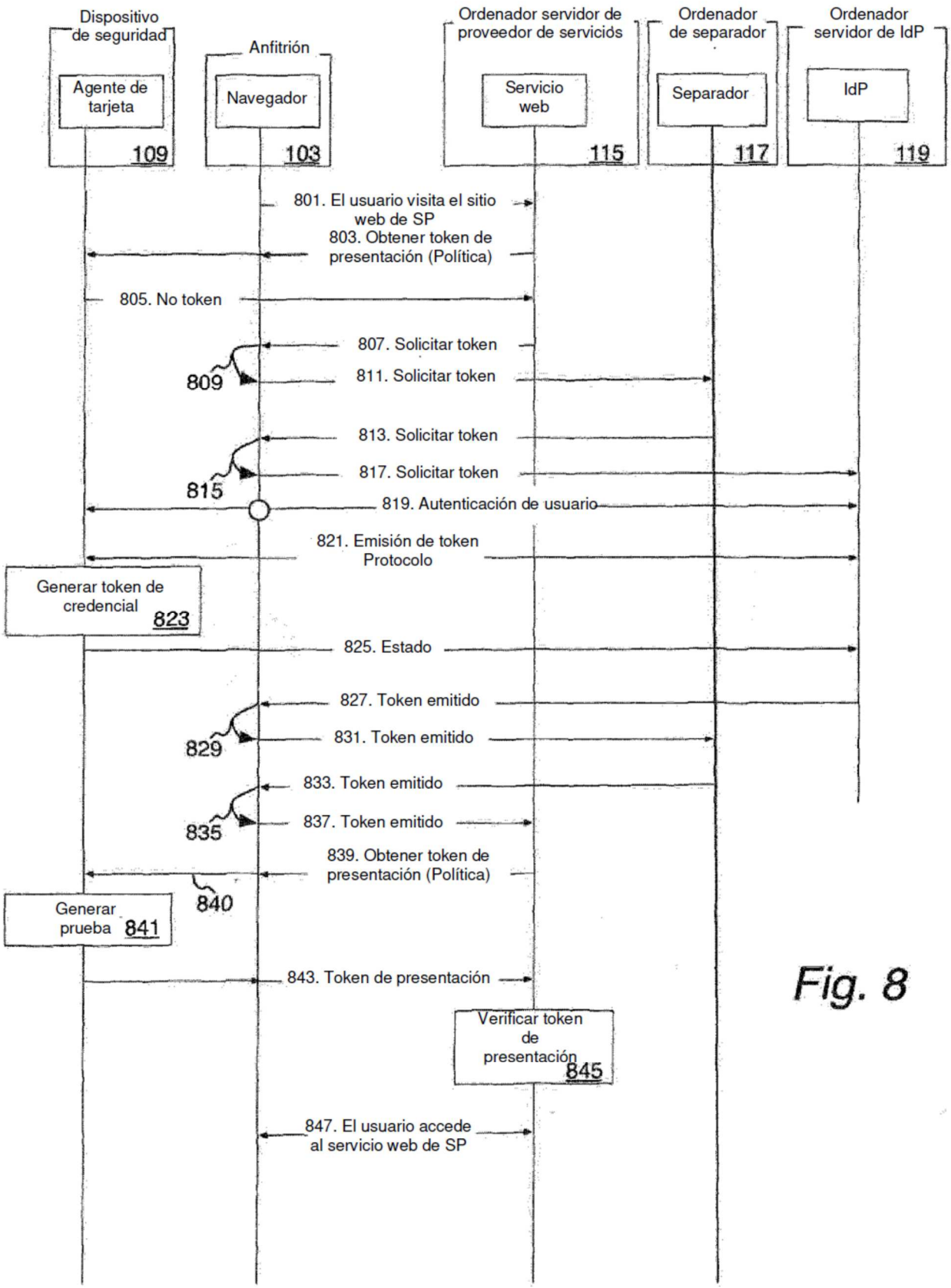
Dispositivo de seguridad
Agente de tarjeta
109
Anfitrión
Navegador
103
Ordenador servidor de proveedor de servicios
Servicio web
115
Ordenador de separador
Separador
117
Ordenador servidor de IdP
IdP
119
801. El usuario visita el sitio web de SP
803. Obtener token de presentación (Política)
805. No token
807. Solicitar token
809
811. Solicitar token
813. Solicitar token
815
817. Solicitar token
819. Autenticación de usuario
821. Emisión de token Protocolo
Generar token de credencial 823
825. Estado
827. Token emitido
829
831. Token emitido
833. Token emitido
835
837. Token emitido
839. Obtener token de presentación (Política)
840
Generar prueba 841
843. Token de presentación
Verificar token de presentación 845
847. El usuario accede al servicio web de SP

Fig. 8

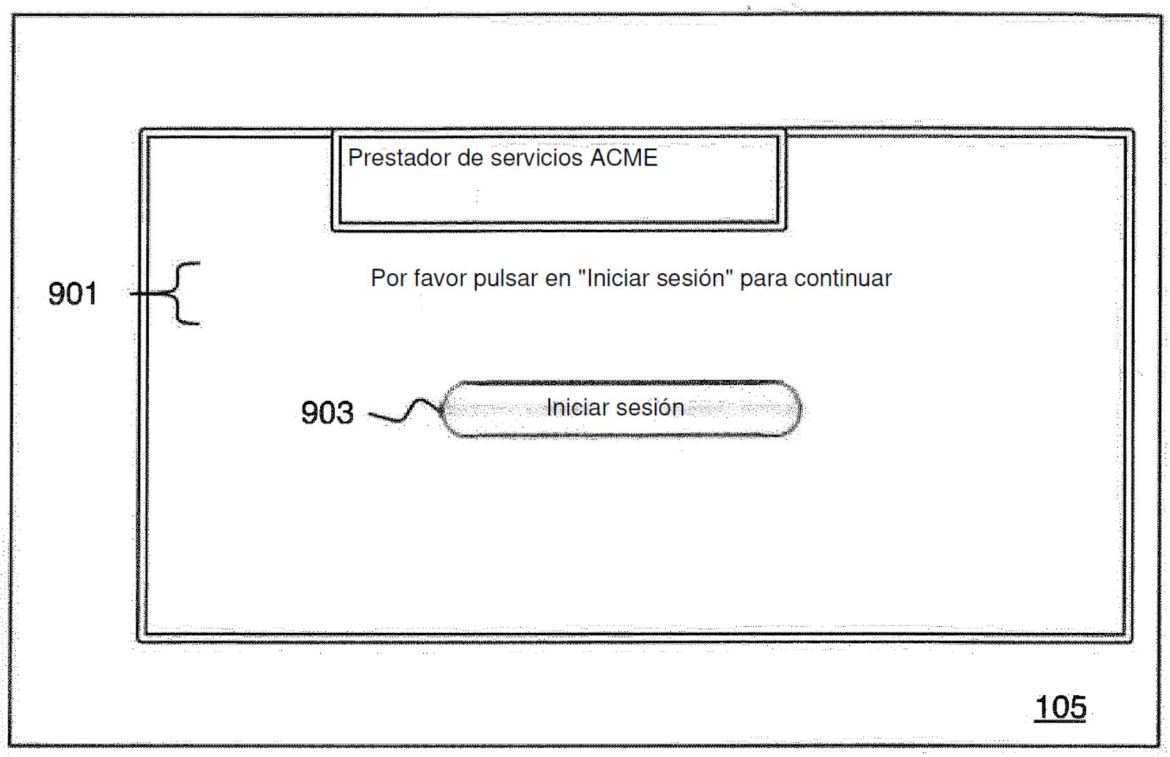
Prestador de servicios ACME
901
Por favor pulsar en "Iniciar sesión" para continuar
903
Iniciar sesión
105

Fig. 9a

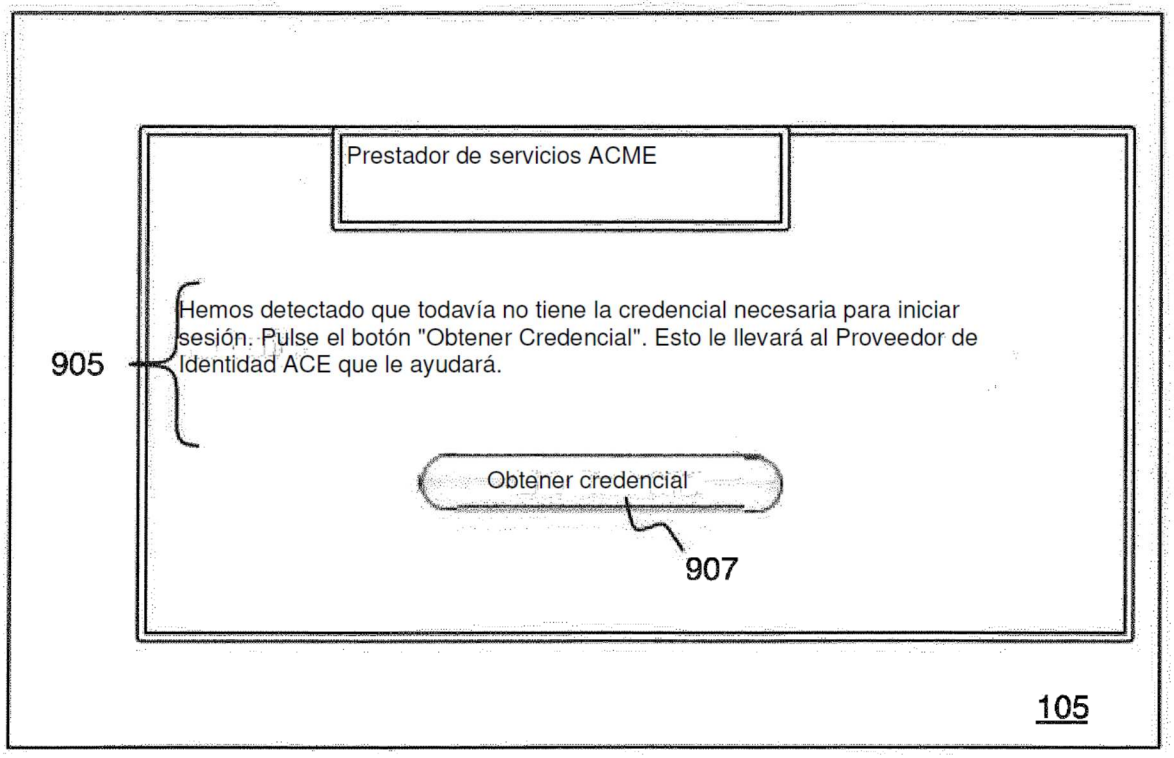
Prestador de servicios ACME
905
Hemos detectado que todavía no tiene la credencial necesaria para iniciar sesión. Pulse el botón "Obtener Credencial". Esto le llevará al Proveedor de Identidad ACE que le ayudará.
Obtener credencial
907
105

Fig. 9b

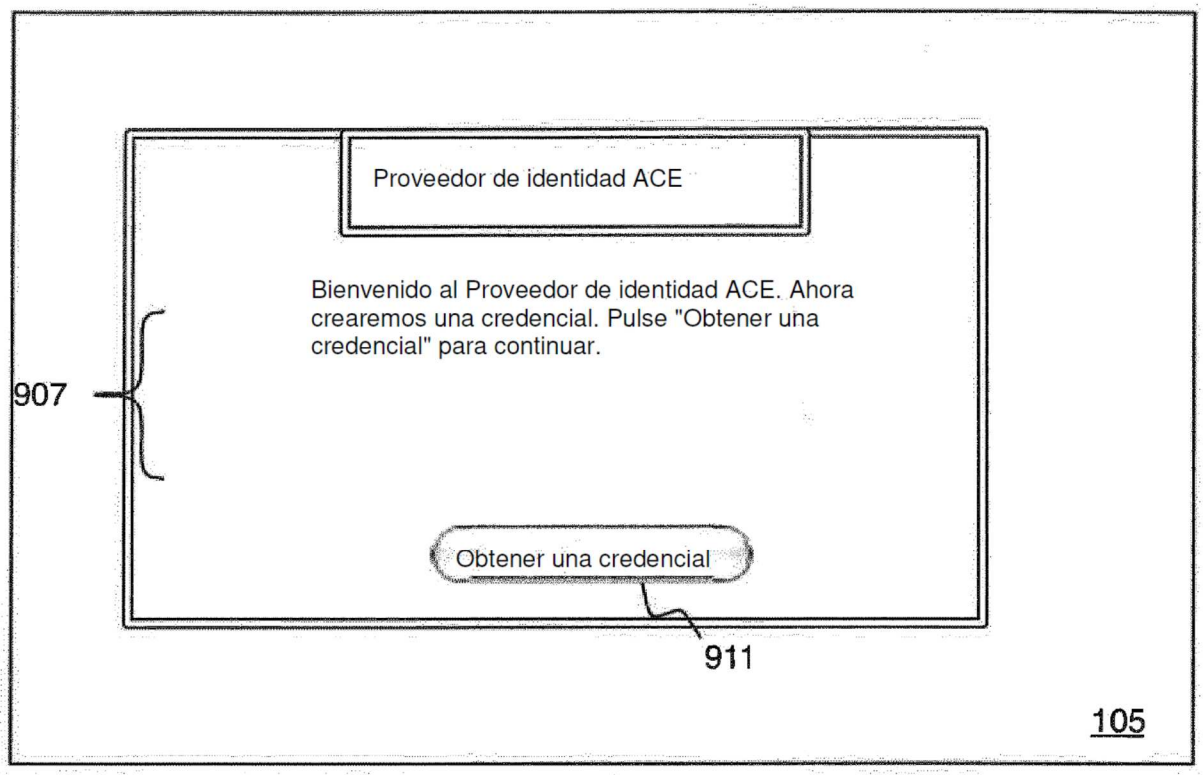
Proveedor de identidad ACE
Bienvenido al Proveedor de identidad ACE. Ahora crearemos una credencial. Pulse "Obtener una credencial" para continuar.
907
Obtener una credencial
911
105

Fig. 9c

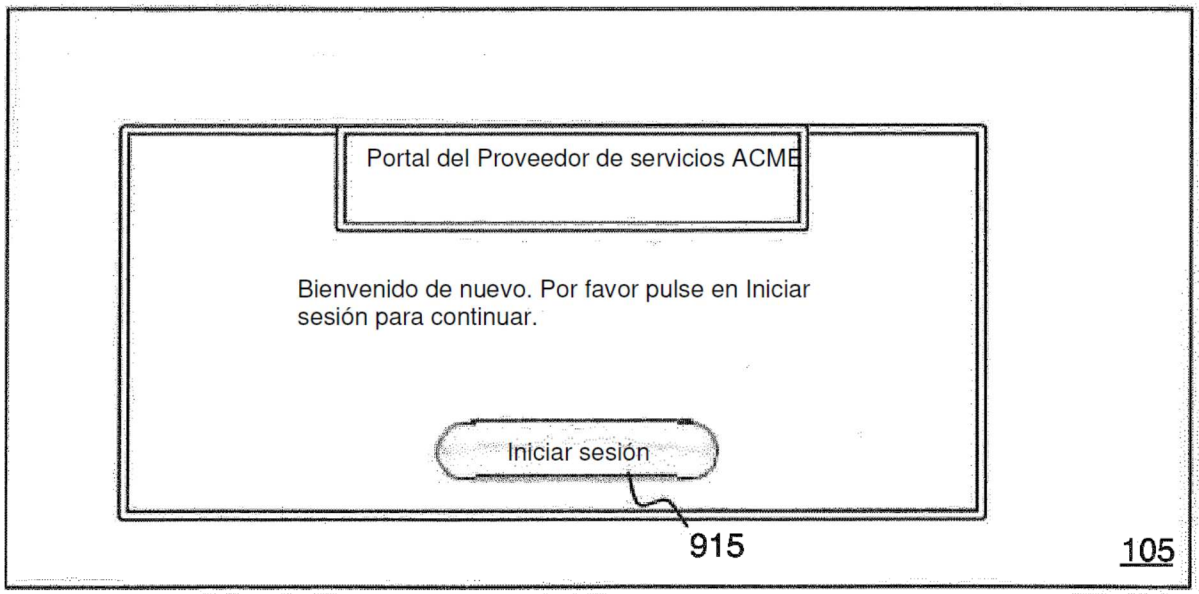
Portal del Proveedor de servicios ACME
Bienvenido de nuevo. Por favor pulse en Iniciar sesión para continuar.
Iniciar sesión
915
105

Fig. 9d