(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 750 239**

(51) Int. CI.:

G06F 7/04 (2006.01)
G06F 21/41 (2013.01)
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: **10.11.2009 PCT/US2009/063845**

(87) Fecha y número de publicación internacional: **20.05.2010 WO10056655**

(96) Fecha de presentación y número de la solicitud europea: **10.11.2009 E 09826615 (8)**

(97) Fecha y número de publicación de la concesión europea: **28.08.2019 EP 2353080**

(54) Título: **Método y sistema para proporcionar un servicio de autenticación federado con expiración gradual de credenciales**

(30) Prioridad:

13.11.2008 US 270486

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.03.2020

(73) Titular/es:

ONESPAN INTERNATIONAL GMBH (100.0%)
World-Wide Business Center, Balz-Zimmermannstrasse 7
8152 Glattbrugg, CH

(72) Inventor/es:

NOE, FREDERICK

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Método y sistema para proporcionar un servicio de autenticación federado con expiración gradual de credenciales

Campo técnico

La presente invención se refiere al campo de la autenticación de usuarios de servicios a través de una red informática, más en concreto dentro del paradigma de la autenticación federada.

Antecedentes de la técnica

La autenticación federada es una arquitectura de servicio diseñada para mejorar la capacidad de gestión y la experiencia del usuario de entornos de aplicación de red que operan bajo una relación de muchos a muchos entre el conjunto de usuarios y el conjunto de aplicaciones. La manifestación práctica de una plataforma de autenticación federada es la capacidad de realizar un Inicio de Sesión Único (SSO), es decir, permitiendo que un usuario inicie sesión en una pluralidad de aplicaciones de red sin requerirle que introduzca credenciales cada vez que este cruce la frontera virtual entre diferentes dominios administrativos.

Un concepto central en la autenticación federada es la agrupación de diversos proveedores de servicios (estos se pueden materializar como servidores individuales, o como diferentes aplicaciones en el mismo servidor) en una federación que se basa en un proveedor de identidad común. Cualquier solicitud de autenticación de un usuario nuevo es procesada por el autenticador común, que emite un "vale". Este vale constituye una aserción del autenticador común acerca de la identidad del usuario y, en algunas realizaciones, acerca de la entidad de certificación asociada del usuario para acceder a servicios dentro de la federación. El vale se puede presentar subsiguientemente a diferentes proveedores de servicios dentro de la misma federación. El vale tiene una vigencia limitada; este puede o bien expirar de forma automática (después de la expiración de una cantidad predefinida de tiempo), o bien expirar como el resultado de una acción explícita (por ejemplo, cerrando el usuario la sesión de la federación, o una revocación de vale iniciada por el autenticador común). Tal expiración del vale es independiente de la expiración de una sesión de inicio de sesión en un servidor particular, que requiere que el usuario inicie sesión de nuevo.

En la técnica se conocen varias variaciones de esquemas de autenticación federada. Por ejemplo, el documento US 6 892 307 divulga un marco de trabajo de inicio de sesión único (SSO) con una correlación de los niveles de confianza con los requisitos de autenticación que se ve influenciada por información de entorno tal como el instante de la solicitud y el documento XP019205701 divulga un sistema de autenticación y de control de acceso basándose en un nivel de confianza que se ajusta de forma dinámica considerando información de contexto tal como el instante. La patente de EE. UU. 6.668.322 [el documento US 6668322 B (Wood, David et al.)] divulga un sistema y método de gestión de acceso que emplea credenciales seguras. El método incluye autenticar a un usuario final (cliente) por medio de una credencial de inicio de sesión, y emitir credenciales de sesión criptográficamente aseguradas que se pueden usar para obtener acceso a una pluralidad de recursos de información, con lo que tal verificación no requiere conocimiento de la clave con la que se generó la credencial de sesión. Esta forma de asegurar criptográficamente la credencial de sesión prevé una arquitectura por medio de la cual una infraestructura de autenticación centralizada emite las credenciales de sesión, pero una nube descentralizada de proveedores de aplicaciones es capaz de verificar de forma autónoma estas credenciales de sesión. Wood et al. también divulgan una vigencia finita de acuerdo con las credenciales de sesión criptográficamente aseguradas. Wood et al. divulgan adicionalmente emitir diferentes credenciales de sesión criptográficamente aseguradas asociadas con diferentes niveles de confianza, que dan acceso a diferentes recursos de información, notablemente para proporcionar la posibilidad de proteger recursos más sensibles con una forma más fuerte de autenticación.

La publicación de patente de EE. UU. n.º 2002/0184507A1 [el documento US 2002184507 A (Makower, David et al.) 05-12-2002] divulga un método y sistema de inicio de sesión único centralizado para un entorno de cliente - servidor, que se centra más en concreto en las interacciones de protocolo de transferencia de hipertexto (http), es decir, una solución de "inicio de sesión único web". En esa arquitectura, "los usuarios se autentican a sí mismos con uno cualquiera de un grupo de servidores federados, cada servidor federado se comunica con el servidor de inicio de sesión central de tal modo que un usuario con una sesión actual no necesita volver a ser autenticado por otros servidores en la federación". El esquema implica una redirección de http de la aplicación de servidor a la que se desea acceder (el "servidor de origen"), a un servidor de inicio de sesión central, y de vuelta al servidor de origen. La primera instrucción de redirección incluye un desafío generado por el servidor de origen. El servidor de inicio de sesión central busca en primer lugar una indicación de si el cliente ha establecido ya una sesión, lo que se podría señalizar mediante la presencia de una "cookie" de http. Si no se ha establecido por adelantado sesión alguna, el inicio de sesión central genera una "cookie" nueva, y redirige al cliente de vuelta al servidor de origen (incluyendo el desafío del servidor de origen con las instrucciones de redirección). El cliente redirigido se autenticará entonces con el servidor de origen, que conserva un registro de la sesión establecida de este modo, e informa al servidor de inicio de sesión central de esta sesión de una forma segura (usando una comunicación firmada y cifrada). La sesión tiene una vigencia finita. Siempre que la sesión sea válida, cualquier solicitud subsiguiente de los mismos clientes para acceder a otros servidores en la federación se redirigirá del servidor de inicio de sesión central a los servidores de origen respectivos, con una firma sobre los datos de identificación de sesión relevantes y el desafío del servidor de origen para confirmar que se ha

establecido ya una sesión válida con al menos un servidor federado. Tras ser informado del establecimiento de cada sesión subsiguiente en cualquier servidor federado, el servidor de inicio de sesión central actualiza el tiempo de expiración de la sesión relevante del cliente. A la inversa, el servidor de inicio de sesión central puede, tras una solicitud del cliente retransmitida por un servidor federado, terminar activamente una sesión existente, y propagar esta finalización hacia todos los servidores federados en los que siguen estando activas sesiones locales.

En la patente de EE. UU. 7.194.547 [el documento US 7194547 B (Moreh, Jahanshah et al.) 20-03-2007], se divulga un servicio de autenticación federado que permite que los clientes se autentiquen a través de una diversidad de mecanismos de autenticación. En esa arquitectura, se usa un intermediario de protocolo para traducir y retransmitir las credenciales del cliente a un mecanismo de autenticación apropiado, y para generar, tras una autenticación con éxito, una "aserción de nombre" que puede ser usada por el cliente para acceder a una aplicación de servidor. En el método de acuerdo con Moreh et al., el cliente inicia el proceso de obtener acceso a la aplicación de servidor al entrar en contacto con un agente de autenticación y trasladarle la identidad y el dominio relevantes del cliente. El agente de autenticación proporciona información acerca de un mecanismo de autenticación para su uso por el cliente. El cliente comunica entonces una solicitud de autenticación para acceder a la aplicación de servidor a un intermediario de protocolo. El intermediario de protocolo recibe la solicitud de autenticación del cliente y la traduce al protocolo nativo del mecanismo de autenticación apropiado. El intermediario de protocolo intenta autenticarse con el mecanismo de autenticación y, tras una autenticación con éxito, el intermediario de protocolo recibe de vuelta del mecanismo de autenticación una respuesta que incluye atributos y derechos de acceso del cliente. El intermediario de protocolo crea entonces una aserción de nombre y, opcionalmente, unos derechos, que traduce a una respuesta de autenticación transmitida de vuelta al cliente. El tiempo de expiración de la aserción de nombre puede ser solicitado por el cliente, la aplicación de servidor, o el mecanismo de autenticación. El cliente entrega la respuesta de autenticación a la aplicación de servidor.

La ventaja básica de un sistema de inicio de sesión único es que un usuario solo se autentica una vez. Después de una autenticación con éxito en el sistema de inicio de sesión único central, el sistema central dará lugar a que el usuario inicie sesión de forma automática en otros sistemas. Después de una cantidad configurada de tiempo desde la última actividad de usuario en la sesión, la sesión de autenticación en el sistema de inicio de sesión único expira y el usuario se ha de volver a autenticar.

En muchos sistemas de inicio de sesión único, cada tipo de autenticación tiene un nivel de confianza de autenticación asociado. Las aplicaciones integradas con estos sistemas de inicio de sesión único definirán un determinado nivel de confianza de autenticación requerido. Los usuarios de una aplicación de este tipo necesitarán ser autenticados al nivel de confianza de autenticación definido o mejor, antes de que se les permita usar esa aplicación.

Divulgación de la invención

Problema técnico

En las soluciones de la técnica anterior, una vez que un usuario se ha autenticado a un determinado nivel de confianza de autenticación, el nivel de confianza de autenticación permanece constante durante la totalidad de la sesión de inicio de sesión único. El nivel de confianza solo se puede aumentar al volver a autenticarse con el sistema de inicio de sesión único usando un método de autenticación que representa un nivel de confianza diferente.

Este modelo no aborda de forma adecuada el hecho de que el valor de seguridad de una autenticación con éxito disminuye con el paso del tiempo. Los sistemas de inicio de sesión único como se conocen en la técnica tienen un tiempo de expiración, lo que protege a los sistemas federados frente a que se acceda a los mismos por medio de una sesión de inicio de sesión único que ya no está bajo el control del usuario legítimo o que ha sido puesto en peligro en el sentido criptográfico, riesgos que aumentan a medida que pasa el tiempo. Los sistemas de inicio de sesión único que soportan diferentes niveles de confianza deberían tener más confianza en una autenticación reciente que en una menos reciente.

Solución técnica

La presente invención se basa en la idea de que el problema de seguridad descrito anteriormente se puede abordar de forma adecuada en los sistemas de inicio de sesión único de múltiples niveles mediante la introducción de una degradación de nivel de confianza de autenticación.

Una idea para superar los problemas especificados anteriormente es implementar en el sistema de inicio de sesión único un algoritmo que realiza una degradación de nivel de confianza de autenticación. De esta forma, el sistema de inicio de sesión único solo permitirá a un usuario autenticado acceder a un determinado recurso si el nivel de confianza de autenticación actual es igual a o mayor que el nivel de confianza de autenticación requerido para el recurso.

El nivel de confianza de autenticación instantáneo L(t) será igual a o menor que el nivel de confianza de autenticación inicial L_0 y se calculará basándose en las reglas de degradación de nivel de confianza de autenticación configuradas.

Son posibles diferentes algoritmos para implementar esta degradación de nivel de confianza de autenticación.

Un algoritmo de este tipo proporciona una degradación lineal: en este caso, el nivel de confianza de autenticación disminuye proporcionalmente al tiempo *t* transcurrido desde el momento de la autenticación con éxito:

$$L(t) = \text{máx}\ \{0, L_0\ (1 - c\ t)\}$$

Otro algoritmo de este tipo proporciona una degradación basada en escalones: en este caso, el nivel de confianza de autenticación disminuye en función del tiempo transcurrido desde la autenticación con éxito, en uno o más escalones discretos.

En algunas realizaciones, el ritmo o la cantidad de degradación del nivel de confianza podría ser una función del grado de actividad de usuario. Por ejemplo, si el usuario permanece inactivo durante una determinada cantidad de tiempo, el nivel de confianza actual se puede degradar a un determinado nivel configurado que es menor que el nivel de confianza actual.

El experto en la materia entenderá que hay innumerables otros algoritmos que se podrían usar para lograr el mismo fin, sin apartarse del ámbito de la invención.

La evaluación del nivel de confianza en cualquier momento dado puede tener lugar de diversas formas. En una realización posible, la evaluación se realiza en el servidor de autenticación, posiblemente cada vez que se recibe una solicitud de autenticación. Por lo tanto, el servidor de autenticación devolverá, en un vale, el nivel de confianza más actual asociado con una sesión activa. En otra realización posible, el algoritmo de degradación es conocido por el servidor que proporciona el recurso. Se puede usar el mismo vale de autenticación de principio a fin de la sesión, pero este se vuelve de menor confianza a medida que pasa el tiempo, hasta que el nivel de confianza disminuye por debajo del nivel de confianza mínimo requerido para el recurso en cuestión, instante en el que ya no se puede seguir usando para conseguir acceso a dicho recurso. Una forma híbrida de implementar esto es dejar que el servidor de autenticación emita un "vale en capas", cada capa del cual es un vale con un determinado nivel de confianza y un tiempo de expiración asociado, en donde las capas con unos niveles de confianza más altos se ajustan para expirar antes que las capas con unos niveles de confianza más bajos. También es posible implementar un mecanismo de doble comprobación, en el que tanto el servidor de autenticación como el servidor que proporciona el recurso realizan una evaluación de acuerdo con un algoritmo de degradación. En una realización particular, el servidor que proporciona el recurso puede aplicar su propia versión del algoritmo de degradación.

Efectos ventajosos

En las soluciones de la técnica anterior, una vez que un usuario se ha autenticado a un determinado nivel de confianza de autenticación, el nivel de confianza de autenticación permanece constante durante la totalidad de la sesión de inicio de sesión único. El tiempo de expiración de la credencial está vinculado con el nivel de confianza proporcionado por la credencial; habitualmente, un nivel de confianza alto está vinculado con un tiempo de expiración corto, lo que implica que una autenticación de alto nivel puede requerir volver a autenticarse frecuentemente.

La presente invención proporciona un mecanismo para permitir que el nivel de confianza disminuya sin volver a autenticarse con el sistema de inicio de sesión único, bajando hasta el nivel al que ya no es suficiente para obtener acceso a un recurso deseado. En ese punto en el tiempo, el usuario vuelve a autenticarse.

De esta forma, los usuarios que realizan una autenticación inicial de alta calidad pueden ser dotados de credenciales que tienen una vigencia larga para recursos menos sensibles mientras que, al mismo tiempo, la seguridad de recursos sensibles específicos se puede mantener a un nivel alto debido a que estas credenciales de larga duración se degradarían con relativa rapidez por debajo del nivel de confianza alto requerido para estos recursos sensibles. Por lo tanto, la invención proporciona un equilibrio mejorado entre asegurar el acceso a recursos sensibles y mantener la comodidad para los usuarios, en especial para recursos menos sensibles.

Breve descripción de los dibujos

Las anteriores y otras características y ventajas de la presente invención serán evidentes a partir de la siguiente descripción, más concreta, de varias realizaciones de la invención, como se ilustra en los dibujos adjuntos.

La figura 1 muestra un diagrama de flujo del método de acuerdo con la invención, que ilustra las etapas realizadas por un cliente, un servidor, un servicio de inicio de sesión único y la memoria caché de autenticación de dicho servicio.
La figura 2 muestra un diagrama de interacción de protocolo del método de acuerdo con la invención, que ilustra las interacciones de un cliente 10, un primer servidor 20, un servicio de inicio de sesión único 30, la memoria caché 40 del servicio y un segundo servidor 50.

Se usan las mismas etiquetas tanto en la figura 1 como en la figura 2 para designar los mismos actos y características,

o unos conceptualmente similares.

La figura 3 proporciona una ilustración esquemática de un sistema 301 que proporciona las funciones de un servidor de autenticación de acuerdo con la invención.

Modo o modos para llevar a cabo la invención

En un método de acuerdo con la presente invención, un usuario final 10 que intenta acceder a un recurso protegido en un servidor 20, protegido por un sistema de autorización, pasaría a través de las siguientes etapas.

Tras solicitar acceso al recurso 101, el usuario final es redirigido 102 a un servicio de autenticación de SSO para iniciar sesión. Por medio del mensaje de redirección 102 y la solicitud 103 subsiguiente del cliente, el sistema 20 proporciona al servicio de autenticación 30 una indicación del nivel de confianza de autenticación mínimo para el recurso protegido solicitado. En su interacción 103 con el servicio de autenticación 30, el usuario final 10 proporciona las credenciales de autenticación necesarias. El servicio de autenticación 30 verifica las credenciales de autenticación y devuelve 104a un vale de autenticación que contiene una identificación del usuario autenticado, el nivel de confianza de autenticación obtenido, un identificador de vale único y, opcionalmente, la identidad o ubicación del servicio de autenticación. El servicio de autenticación 30 guarda una copia del vale de autenticación en su memoria caché 104b.

En una etapa 105 siguiente, el usuario final 10 proporciona este vale al sistema de autorización 20 del servidor. El sistema de autorización 20 verifica este vale con el servicio de autenticación 30 que solicita el nivel de confianza de autenticación 106 actual. El servicio de autenticación 30 consulta su memoria caché 40 para examinar el vale de autenticación, lo que implica una solicitud 107 y una respuesta 108a. Si se halla un vale, el servicio de autenticación 30 calcula 108b el nivel de confianza de autenticación para el usuario 10 especificado usando las reglas de degradación de nivel de confianza de autenticación configuradas y lo devuelve 109 al servicio de autorización 20. Si no se halla vale alguno, el servicio de autenticación 30 devuelve 109 que el nivel de confianza de autenticación es 0. Esto puede ser debido a la expiración de un vale.

El servicio de autorización 20 comprueba si el nivel de confianza de autenticación actual es igual a o mayor que el nivel solicitado y proporciona al usuario final 10 acceso al recurso solicitado si el vale es adecuado 110.

Un intento de acceso subsiguiente a un recurso diferente en la federación se beneficiará de la autenticación realizada en la sesión anterior. Considérese que el mismo usuario final 10 intenta acceder a otro recurso protegido en un segundo servidor 50, protegido por un sistema de autorización.

El usuario final 10 proporciona su vale 111 obtenido anteriormente, al sistema de autorización 50. El sistema de autorización 50 verifica este vale con el servicio de autenticación 30 que solicita el nivel de confianza de autenticación 112 actual. El servicio de autenticación 30 busca el vale de autenticación en su memoria caché, lo que implica la solicitud 113 y la respuesta 114. Si se halla un vale, el servicio de autenticación 30 calcula el nivel de confianza de autenticación para el usuario 10 especificado usando las reglas de degradación de nivel de confianza de autenticación configuradas y otra información, tal como el instante en el que se generó el vale, y lo devuelve 115 al servicio de autorización 50. Si no se halla vale alguno, el servicio de autenticación 30 devuelve 115 que el nivel de confianza de autenticación es 0. Esto puede ser debido a la expiración de un vale.

El servicio de autorización 50 comprueba si el nivel de confianza de autenticación actual es igual a o mayor que el nivel solicitado y proporciona al usuario final 10 acceso al recurso solicitado si el vale es adecuado 116.

En un esquema alternativo, una solicitud de usuario 101 que incluye un vale es manejada por el servidor 20, sin interacción adicional con el servidor de autenticación 30. Esto es posible si el vale se encuentra en una forma que se pueda verificar localmente; este puede ser el caso si el servidor 20 comparte un secreto criptográfico con el servidor de autenticación 30, o si el servidor de autenticación 30 usa una infraestructura de clave pública para generar el vale. En este esquema, los mensajes 101 y 105 del usuario coinciden en la práctica. El intercambio caracterizado por los mensajes 106, 107, 108a y 109 se sustituye por un procesamiento local en el servidor 20, que incluye evaluar el nivel de confianza actual para el usuario 10 usando las reglas de degradación de nivel de confianza de autenticación configuradas y otra información, tal como el instante en el que se generó el vale. El servidor 20 proporciona al usuario final 10 acceso al recurso solicitado si el vale es adecuado 110.

Una realización general del método para proporcionar un servicio de inicio de sesión único comprende recibir, en un servidor de autenticación, una solicitud de autenticación de un usuario; autenticar a dicho usuario en dicho servidor de autenticación; asociar al menos un nivel de confianza inicial con dicha autenticación; recibir una solicitud de validación en relación con dicho usuario y un servidor de aplicaciones, imponiendo dicho servidor de aplicaciones un nivel mínimo de confianza requerido; calcular un nivel de confianza actualizado que se va a asociar con dicha autenticación a partir de al menos una función del tiempo; conceder a dicho usuario acceso a dicho servidor de aplicaciones si dicho nivel de confianza actualizado supera dicho nivel mínimo requerido.

En una realización de la presente invención, el método comprende adicionalmente generar un vale de autenticación

para dicho usuario. En una realización particular del método de la presente invención, dicha solicitud de validación contiene una referencia a dicho vale de autenticación.

Otra realización general del método para proporcionar un servicio de inicio de sesión único comprende recibir, en un servidor de autenticación, una solicitud de autenticación de un usuario; autenticar a dicho usuario en dicho servidor de autenticación; generar un vale de autenticación para dicho usuario; asociar al menos un nivel de confianza inicial con dicho vale de autenticación; recibir una solicitud de validación en relación con dicho usuario y un servidor de aplicaciones, conteniendo dicha solicitud de validación una referencia a dicho vale de autenticación, e imponiendo dicho servidor de aplicaciones un nivel mínimo de confianza requerido; calcular un nivel de confianza actualizado que se va a asociar con dicho vale de autenticación a partir de al menos una función del tiempo; conceder a dicho usuario acceso a dicho servidor de aplicaciones si dicho nivel de confianza actualizado supera dicho nivel mínimo requerido.

En una realización del método de la presente invención, dicha función del tiempo es una función del tiempo transcurrido desde dicha autenticación.

En otra realización del método de la presente invención, dicho cálculo también usa dicho nivel de confianza inicial.

En aún otra realización del método de la presente invención, dicho cálculo también usa dicho nivel mínimo de confianza requerido, y dicho cálculo da como resultado un valor simbólico que indica un fallo de autenticación si no se concede dicho nivel mínimo de confianza requerido.

En una realización adicional del método de la presente invención, dicha recepción de dicha solicitud de validación tiene lugar en dicho servidor de aplicaciones. En aún otra realización adicional del método de la presente invención, dicha recepción de dicha solicitud de validación tiene lugar en dicho servidor de autenticación.

En una realización del método de la presente invención, dicho cálculo comprende disminuir dicho nivel de confianza actualizado de forma lineal con el tiempo. En otra realización del método de la presente invención, dicho cálculo comprende disminuir dicho nivel de confianza actualizado de forma exponencial con el tiempo. En otra realización del método de la presente invención, dicho cálculo comprende disminuir dicho nivel de confianza actualizado como una serie de funciones escalón en el dominio del tiempo.

En una realización del método de la presente invención, dicho cálculo comprende verificar un tiempo de expiración para una pluralidad de niveles de confianza inicialmente asociados con dicho vale.

En una realización del método de la presente invención, dicho cálculo tiene lugar en dicho servidor de aplicaciones. En otra realización del método de la presente invención, dicho cálculo tiene lugar en dicho servidor de autenticación.

En otra realización del método de la presente invención, dicho nivel mínimo de confianza requerido puede variar en diferentes servidores de aplicaciones. En general, un nivel de confianza aplicable en un servidor de aplicaciones es independiente de un nivel de confianza aplicable en otro servidor de aplicaciones.

Una realización general del sistema 301 para proporcionar un servicio de inicio de sesión único comprende un primer agente de recepción 302 para recibir una solicitud de autenticación de un usuario; un agente de autenticación 303 para autenticar a dicho usuario; un agente de emisión 304 para emitir un vale de autenticación para dicho usuario, en donde al menos un nivel de confianza inicial está asociado con dicho vale de autenticación; un segundo agente de recepción 305 para recibir una solicitud de validación en relación con dicho usuario a partir de un servidor de aplicaciones, conteniendo dicha solicitud una referencia a dicho vale de autenticación, e imponiendo dicho servidor de aplicaciones un nivel mínimo de confianza requerido; un procesador 306 para calcular un nivel de confianza actualizado que se va a asociar con dicho vale de autenticación a partir de al menos una función del tiempo; y un agente de envío 307 para enviar una señal indicativa de dicho cálculo a dicho servidor de aplicaciones.

En una realización, los elementos 302 - 307 se materializan en un servidor de autenticación de SSO que se puede implementar como un ordenador de propósito general dotado de software o firmware para implementar estas funciones específicas. El primer agente de recepción responde a solicitudes de autenticación de usuarios al almacenar la solicitud y trasladar esa información al agente de autenticación. El agente de autenticación puede determinar si el usuario es o se debería considerar auténtico basándose en la información recibida en la solicitud (y quizá otra información, o bien disponible para el agente de autenticación o bien obtenida del usuario en respuesta a una o más solicitudes específicas generadas por el agente de autenticación). Los procedimientos para autenticar al usuario son convencionales. Si se considera que el usuario es auténtico, el agente de autenticación puede realizar entradas apropiadas en un almacenamiento (o bien local o bien global) y trasladar entonces esta información al agente de emisión. El agente de emisión manifiesta la aprobación al usuario y quizá proporciona una cierta indicación tangible de esa aprobación al usuario. El segundo agente de recepción recibe solicitudes de validación a partir de servidores de aplicaciones. La solicitud de validación incluye o se refiere a la autenticación previamente relacionada con el usuario. El segundo agente de recepción trasladará esta información al procesador, que puede calcular un nivel de confianza actualizado asociado con la autenticación. El procesador traslada entonces este nivel de confianza actualizado al agente de envío que traslada la información al destino apropiado tal como el servidor de aplicaciones que realizó la solicitud de validación.

En una realización del sistema de la presente invención, dicha función del tiempo es una función del tiempo transcurrido desde dicha autenticación.

En otra realización del sistema de la presente invención, dicho cálculo también usa dicho nivel de confianza inicial.

En aún otra realización del sistema de la presente invención, dicho cálculo también usa dicho nivel mínimo de confianza requerido, y dicho cálculo da como resultado un valor simbólico que indica un fallo de autenticación si no se concede dicho nivel mínimo de confianza requerido.

En una realización del sistema de la presente invención, dicho cálculo comprende disminuir dicho nivel de confianza actualizado de forma lineal con el tiempo. En otra realización del sistema de la presente invención, dicho cálculo comprende disminuir dicho nivel de confianza actualizado de forma exponencial con el tiempo. En aún otra realización del sistema de la presente invención, dicho cálculo comprende disminuir dicho nivel de confianza actualizado como una serie de funciones escalón en el dominio del tiempo.

En una realización del sistema de la presente invención, dicho cálculo comprende verificar un tiempo de expiración para cada uno de dichos al menos un niveles de confianza.

Una realización general del sistema para proporcionar un servicio de inicio de sesión único comprende un agente de recepción para recibir una solicitud de autenticación de un usuario; un agente de autenticación para autenticar a dicho usuario; y, un agente de emisión para emitir un vale de autenticación para dicho usuario, en donde al menos un nivel de confianza inicial y al menos un nivel de confianza subsiguiente están asociados con dicho vale de autenticación, teniendo dicho nivel de confianza subsiguiente un periodo de validez que se extiende más allá del periodo de validez de dicho nivel de confianza inicial.

En una realización de la presente invención, el sistema comprende adicionalmente un primer servidor y un segundo servidor, incluyendo cada uno de dichos servidores un agente de confianza, estableciendo cada agente de confianza un nivel mínimo de confianza, que es independiente del nivel de confianza de otro agente de confianza.

Una realización general del método para proporcionar un servicio de inicio de sesión único comprende recibir una solicitud de autenticación de un usuario; autenticar a dicho usuario; y, emitir un vale de autenticación para dicho usuario, en donde al menos un nivel de confianza inicial y al menos un nivel de confianza subsiguiente están asociados con dicho vale de autenticación, teniendo dicho nivel de confianza subsiguiente un periodo de validez que se extiende más allá del periodo de validez de dicho nivel de confianza inicial.

Los elementos del método y sistemas descritos en el presente documento se pueden implementar en hardware para aplicaciones específicas, hardware programable in situ, procesadores de propósito general con software adecuado, y similares, como resultará evidente al experto en la materia.

Aunque se han descrito anteriormente diversas de las realizaciones de la presente invención, debería entenderse que se han presentado solo a modo de ejemplo, y no como limitación. Por lo tanto, la amplitud y el alcance de la presente invención no deberían estar limitados por ninguna de las realizaciones ilustrativas anteriormente descritas, sino que solo debería definirse de acuerdo con las siguientes reivindicaciones y sus equivalentes.

REIVINDICACIONES

1. Un método para proporcionar un servicio de inicio de sesión único, que comprende

recibir (103), en un servidor de autenticación (30), una solicitud de autenticación de un usuario (10);
autenticar (104a) a dicho usuario (10) en dicho servidor de autenticación (30);
asociar al menos un nivel de confianza inicial con dicha autenticación;
recibir una solicitud de validación (105) en relación con dicho usuario (10) y un servidor de aplicaciones (20), imponiendo dicho servidor de aplicaciones (20) un nivel mínimo de confianza requerido;
calcular (108b) un nivel de confianza actualizado que se va a asociar con dicha autenticación a partir de al menos una función del tiempo;
conceder (109, 110) a dicho usuario (10) acceso a dicho servidor de aplicaciones (20) si dicho nivel de confianza actualizado supera dicho nivel mínimo requerido;
en donde dicha función del tiempo es una función del tiempo transcurrido desde dicha autenticación.

2. El método de la reivindicación 1, que comprende adicionalmente generar un vale de autenticación para dicho usuario.

3. El método de la reivindicación 2, en donde dicha solicitud de validación (105) contiene una referencia a dicho vale de autenticación.

4. El método de cualquiera de las reivindicaciones anteriores, en donde dicho cálculo (108b) también usa dicho nivel de confianza inicial.

5. El método de cualquiera de las reivindicaciones anteriores, en donde dicho cálculo (108b) también usa dicho nivel mínimo de confianza requerido, y en donde dicho cálculo (108b) da como resultado un valor simbólico que indica un fallo de autenticación si no se concede dicho nivel mínimo de confianza requerido.

6. El método de cualquiera de las reivindicaciones 1 - 5, en donde dicho cálculo (108b) comprende disminuir dicho nivel de confianza actualizado de forma lineal o exponencial con el tiempo, o como una serie de funciones escalón en el dominio del tiempo.

7. El método de cualquiera de las reivindicaciones 1 - 5, en donde dicho cálculo (108b) comprende verificar un tiempo de expiración para una pluralidad de niveles de confianza inicialmente asociados con dicha autenticación.

8. El método de cualquiera de las reivindicaciones 1 - 7, en donde dicho cálculo (108b) tiene lugar en dicho servidor de aplicaciones.

9. El método de cualquiera de las reivindicaciones 1 - 7, en donde dicho cálculo (108b) tiene lugar en dicho servidor de autenticación.

10. El método de cualquiera de las reivindicaciones anteriores, en donde dicho nivel mínimo de confianza requerido puede variar en diferentes servidores de aplicaciones (20, 50).

11. El método de cualquiera de las reivindicaciones anteriores, en donde dicho cálculo (108b) de un nivel de confianza actualizado que se va a asociar con dicha autenticación comprende degradar el nivel de confianza de tal modo que el nivel de confianza actualizado es igual a o menor que dicho al menos un nivel de confianza inicial.

12. Un sistema (301) para proporcionar un servicio de inicio de sesión único, que comprende

un primer agente de recepción (302) para recibir una solicitud de autenticación de un usuario (10);
un agente de autenticación (303) para autenticar a dicho usuario (10);
un agente de emisión (304) para emitir un vale de autenticación para dicho usuario (10), en donde al menos un nivel de confianza inicial está asociado con dicho vale de autenticación;
un segundo agente de recepción (305) para recibir una solicitud de validación en relación con dicho usuario (10) a partir de un servidor de aplicaciones (20, 50), conteniendo dicha solicitud una referencia a dicho vale de autenticación, e imponiendo dicho servidor de aplicaciones (20, 50) un nivel mínimo de confianza requerido;
un procesador (306) para calcular un nivel de confianza actualizado que se va a asociar con dicho vale de autenticación a partir de al menos una función del tiempo; y un agente de envío (307) para enviar una señal indicativa de dicho cálculo a dicho servidor de aplicaciones (20, 50);
en donde dicha función del tiempo es una función del tiempo transcurrido desde dicha autenticación.

13. El sistema (301) de la reivindicación 12, en donde dicho cálculo también usa dicho nivel de confianza inicial.

14. El sistema (301) de la reivindicación 12 o la reivindicación 13, en donde dicho cálculo también usa dicho nivel mínimo de confianza requerido, y en donde dicho cálculo da como resultado un valor simbólico que indica un fallo de

autenticación si no se concede dicho nivel mínimo de confianza requerido.

15. El sistema (301) de cualquiera de las reivindicaciones 12 - 14, en donde dicho cálculo comprende disminuir dicho nivel de confianza actualizado de forma lineal o exponencial con el tiempo, o como una serie de funciones escalón en el dominio del tiempo.

16. El sistema (301) de cualquiera de las reivindicaciones 12 - 15, en donde dicho cálculo comprende verificar un tiempo de expiración para cada uno de dichos al menos un niveles de confianza.

17. El sistema (301) de cualquiera de las reivindicaciones 12 - 16, en donde dicho cálculo de un nivel de confianza actualizado que se va a asociar con dicho vale de autenticación comprende degradar el nivel de confianza de tal modo que el nivel de confianza actualizado es igual a o menor que dicho al menos un nivel de confianza inicial.

FIGURA 1

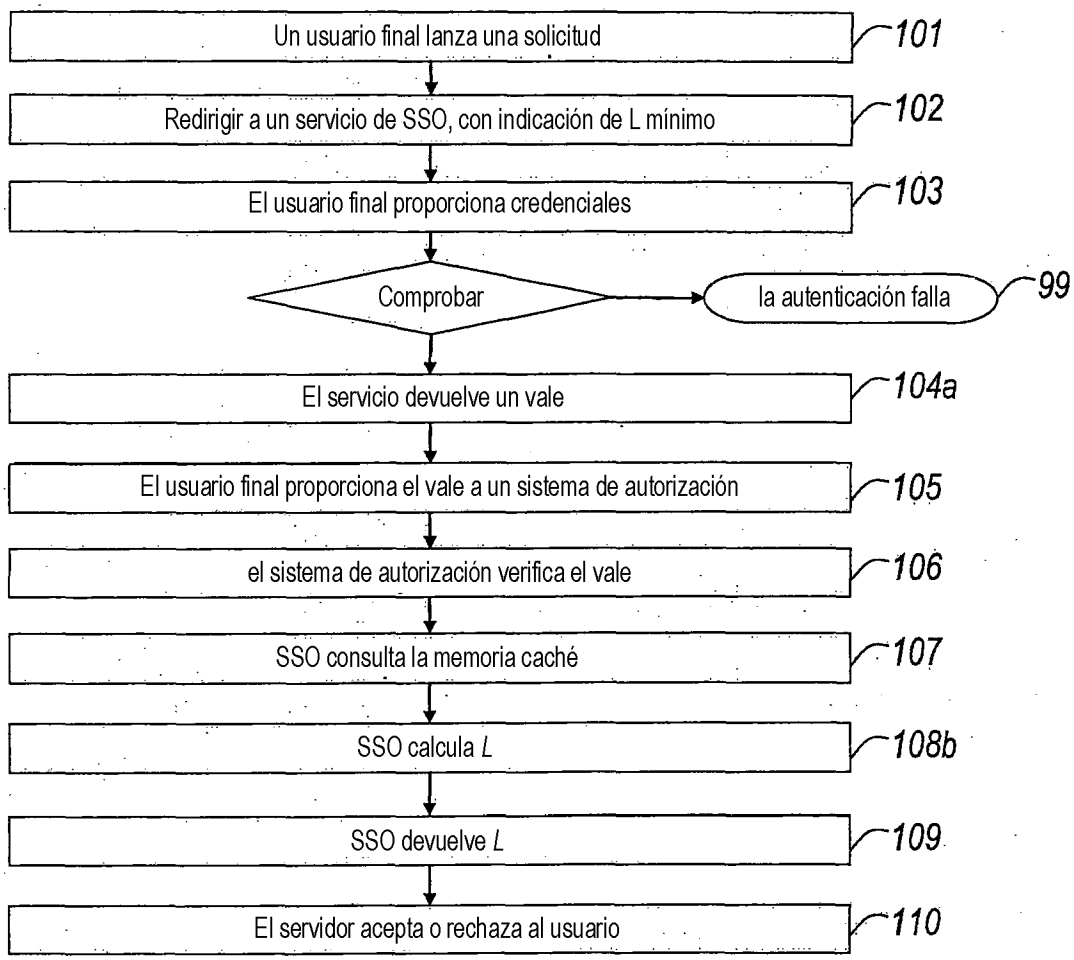
Un usuario final lanza una solicitud
101
Redirigir a un servicio de SSO, con indicación de L mínimo
102
El usuario final proporciona credenciales
103
Comprobar
la autenticación falla
99
El servicio devuelve un vale
104a
El usuario final proporciona el vale a un sistema de autorización
105
el sistema de autorización verifica el vale
106
SSO consulta la memoria caché
107
SSO calcula L
108b
SSO devuelve L
109
El servidor acepta o rechaza al usuario
110

FIGURA 2

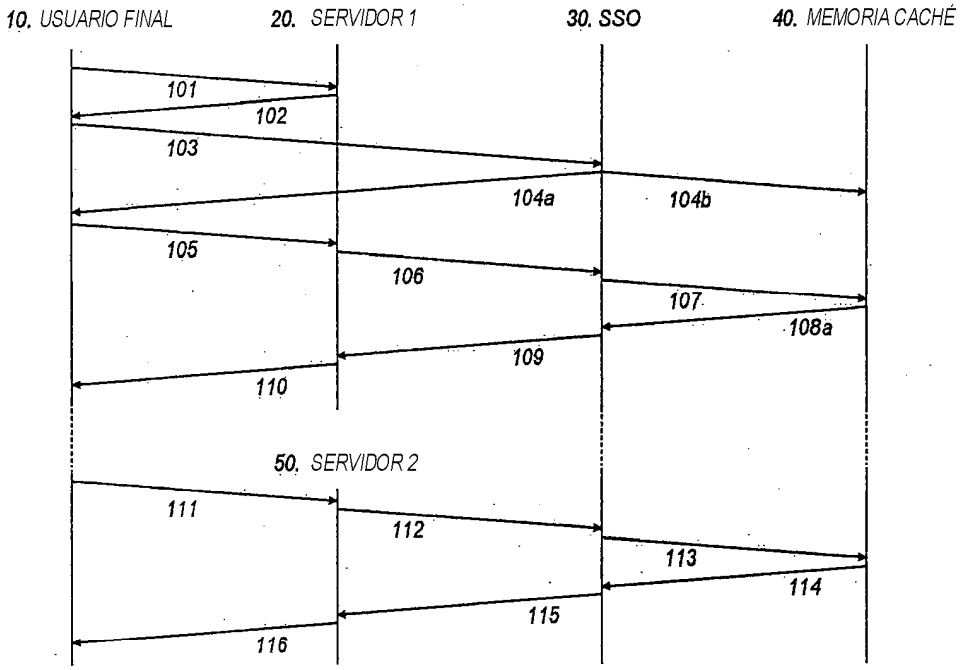

FIGURA 3