(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 816 556**

(51) Int. CI.:

G06F 21/41 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.02.2018 PCT/US2018/017657**

(87) Fecha y número de publicación internacional: **16.08.2018 WO18148568**

(96) Fecha de presentación y número de la solicitud europea: **09.02.2018 E 18707488 (5)**

(97) Fecha y número de publicación de la concesión europea: **22.07.2020 EP 3580679**

(54) Título: **Método, servidor y sistema de inicio de sesión de confianza**

(30) Prioridad:

09.02.2017 CN 201710071568

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.04.2021

(73) Titular/es:

ADVANCED NEW TECHNOLOGIES CO., LTD. (100.0%)
Cayman Corporate Centre, 27 Hospital Road George Town, Grand Cayman KY1-9008, KY

(72) Inventor/es:

YANG, WENXUE

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método, servidor y sistema de inicio de sesión de confianza

Reivindicación de prioridad

Esta solicitud reivindica la prioridad de la Solicitud de Patente China Nº 201710071568.6 presentada el 9 de febrero de 2017.

Campo técnico

La presente solicitud se refiere al campo de las tecnologías de software y, en particular, a un método, servidor y sistema de inicio de sesión de confianza.

Técnica anterior

Con el desarrollo incesante de la ciencia y la tecnología, las tecnologías de software se desarrollan rápidamente, y diversos sistemas de aplicación surgen sin cesar. En un caso general, cuando se utiliza un sistema de aplicación, un usuario necesita ingresar un número de cuenta y una contraseña para implementar un inicio de sesión antes de disfrutar del correspondiente servicio.

Un cliente puede iniciar sesión en un sistema A utilizando un número de cuenta y una contraseña que están registrados en el sistema A; o también puede iniciar sesión en un sistema B confiando en el sistema A utilizando el número de cuenta y la contraseña que están registrados en el sistema A. Cuando un usuario del sistema A inicia sesión en el sistema B confiando en el sistema A, tal manera de inicio de sesión se conoce como inicio de sesión de confianza. Después de iniciar sesión en el sistema B de una manera confiable, el usuario del sistema A puede acceder al servicio correspondiente proporcionado por el sistema B y realizar una operación en el mismo.

En la actualidad, en una solución de inicio de sesión de confianza existente, el sistema B asigna un número de inicio de sesión de confianza al sistema A. A continuación, el sistema A escribe, en una solicitud de inicio de sesión de confianza, parámetros de solicitud de inicio de sesión de usuario en el sistema A y el número de inicio de sesión emitido por el sistema B, cifra la solicitud de inicio de sesión de confianza utilizando una clave y envía la solicitud cifrada. El sistema B descifra la solicitud de inicio de sesión de confianza recibida utilizando una clave pública proporcionada por el sistema A. Después del descifrado, el sistema B comprueba si el número de inicio de sesión de confianza en la solicitud de inicio de sesión de confianza es legal. Si es legal, el usuario del sistema A puede iniciar sesión en el sistema B y el inicio de sesión de confianza es exitoso. Sin embargo, una vez que el inicio de sesión es exitoso con la solución de inicio de sesión de confianza existente, el cliente del sistema A puede acceder a todas las páginas de servicio del sistema B y realizar operaciones en ellas, causando así una amenaza a la seguridad. Por ejemplo, si el robo de una base de datos o el robo de una cuenta se produce en el sistema A (por ejemplo, un sistema de APP de mapas) debido a un requisito de seguridad bajo, el ladrón puede iniciar sesión en el sistema A utilizando la información del usuario obtenida a través del robo de la base de datos o el robo de la cuenta y luego iniciar sesión en el sistema B (por ejemplo, un sistema de APP de pago) a través del sistema A de manera confiable, para realizar una operación en una página (por ejemplo, una página de pago) del sistema B con un requisito de seguridad más alto. Como resultado, el sistema B con un mayor requisito de seguridad se enfrenta a un riesgo.

El documento WO 2011/047722 da a conocer un método llevado a cabo mediante un controlador. El método incluye recibir un mensaje que incluye un simbólico de solicitud. Un simbólico de solicitud es un valor que utiliza un consumidor para solicitar la autorización de un usuario para acceder a recursos protegidos de un proveedor de servicios. Un proveedor de servicios es al menos uno de una aplicación de software y un sitio web que está configurado para proporcionar acceso a recursos protegidos. Un consumidor es al menos uno de una aplicación de software y un sitio web que está configurado para acceder a un proveedor de servicios en nombre de un usuario. El método incluye además determinar si el mensaje cumple con las configuraciones de política que gobiernan el acceso a recursos protegidos; y, si se determina que el mensaje no cumple con la configuración de la política, evitar que el simbólico de solicitud se reenvíe al proveedor de servicios asociado con el simbólico de solicitud.

Resumen de la invención

Las realizaciones de la presente invención proporcionan un método y un aparato de inicio de sesión de confianza, y un dispositivo electrónico, que se utilizan para resolver un problema de seguridad en un inicio de sesión de confianza entre sistemas en la técnica anterior, y mejorar la seguridad del inicio de sesión de confianza. La invención se define en las reivindicaciones.

Un primer aspecto de la presente invención proporciona un método de inicio de sesión de confianza, donde el método se aplica a un primer servidor e incluye:

recibir una solicitud de acceso a la página enviada por un terminal cliente de destino correspondiente a un segundo servidor, utilizándose la solicitud de acceso a la página para solicitar el acceso a una página de servicio proporcionada por el primer servidor;

adquirir un simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página y juzgar si el simbólico de inicio de sesión de confianza temporal tiene un privilegio de servicio para acceder a la página de servicio; y

permitir que el terminal cliente de destino inicie sesión en el primer servidor de manera confiable, si el simbólico de inicio de sesión de confianza temporal tiene el privilegio de servicio para acceder a la página de servicio, y devolver la página de servicio a la que el terminal cliente de destino solicita acceder.

Opcionalmente, el paso de juzgar si el simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página tiene un privilegio de servicio para acceder a la página de servicio incluye:

juzgar si el simbólico de inicio de sesión de confianza temporal y una identificación de servicio de la página de servicio cumplen una primera relación de correspondencia; y

determinar que el simbólico de inicio de sesión de confianza temporal tiene el privilegio de servicio para acceder a la página de servicio, si el simbólico de inicio de sesión de confianza temporal y la identificación de servicio cumplen la primera relación de correspondencia.

Opcionalmente, el paso de juzgar si el simbólico de inicio de sesión de confianza temporal tiene un privilegio de servicio para acceder a la página de servicio incluye:

juzgar si el simbólico de inicio de sesión de confianza temporal y una identificación de servicio de la página de servicio cumplen una primera relación de correspondencia, y juzgar si el simbólico de inicio de sesión de confianza temporal y un identificador de inicio de sesión de confianza actual emitido por el primer servidor al segundo servidor cumplen una segunda relación de correspondencia; y

determinar que el simbólico de inicio de sesión de confianza temporal tiene el privilegio de servicio para acceder a la página de servicio, si el simbólico de inicio de sesión de confianza temporal y la identificación de servicio cumplen la primera relación de correspondencia y el simbólico de inicio de sesión de confianza temporal y el identificador de inicio de sesión de confianza actual cumplen la segunda relación de correspondencia.

Opcionalmente, antes de que el paso de juzgar si el simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página tiene un privilegio servicio para acceder a la página de servicio, el método incluye, además:

juzgar si el simbólico de inicio de sesión de confianza temporal es legal y juzgar si el simbólico de inicio de sesión de confianza temporal expira; y

realizar una operación de juzgar si el simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página tiene un privilegio de servicio para acceder a la página de servicio, si el simbólico de inicio de sesión de confianza temporal es legal y no expira.

Opcionalmente, la página de servicio es una página que se puede cargar al terminal cliente de destino de una manera integrada.

Opcionalmente, el método incluye, además:

recibir una solicitud de adquisición de simbólico enviada por el segundo servidor;

juzgar, en base a la solicitud de adquisición de simbólico, si el terminal cliente de destino es un terminal cliente de confianza;

generar el simbólico de inicio de sesión de confianza temporal si el terminal cliente de destino es un terminal cliente de confianza concedida, y establecer un privilegio de servicio de acceso a la página del simbólico de inicio de sesión de confianza temporal; y

enviar el simbólico de inicio de sesión de confianza temporal al terminal cliente de destino utilizando el segundo servidor.

Opcionalmente, el paso de juzgar, en base a la solicitud de adquisición de simbólico, si el terminal cliente de destino es un terminal cliente de confianza concedida incluye:

juzgar si la solicitud de adquisición de simbólico incluye el identificador de inicio de sesión de confianza actual emitido por el primer servidor al segundo servidor; y

determinar que el terminal cliente de destino es el terminal cliente de confianza otorgada si la solicitud de adquisición de simbólico incluye el identificador de inicio de sesión de confianza actual.

Opcionalmente, el paso de juzgar, en base a la solicitud de adquisición de simbólico, si el terminal cliente de destino es un terminal cliente de confianza concedida incluye:

juzgar si existe un primer terminal cliente correspondiente al terminal cliente de destino en el primer servidor; y

determinar que el terminal cliente de destino es el terminal cliente de confianza concedida si existe el primer terminal cliente.

Un segundo aspecto de la presente invención proporciona un método de inicio de sesión de confianza, donde el método se aplica a un segundo servidor, que es un terminal servidor de un terminal cliente de destino, y el método incluye:

recibir una solicitud de inicio de sesión de confianza enviada por el terminal cliente de destino, utilizándose la solicitud de inicio de sesión de confianza para solicitar iniciar sesión en un primer servidor y acceder a una página de servicio proporcionada por el primer servidor;

generar una solicitud de adquisición de simbólico en base a la solicitud de inicio de sesión de confianza y enviar la solicitud de adquisición de simbólico al primer servidor;

recibir un simbólico de inicio de sesión de confianza temporal retroalimentado por el primer servidor, teniendo el simbólico de inicio de sesión de confianza temporal un privilegio de servicio para iniciar sesión en el primer servidor y acceder a la página de servicio; y

retroalimentar el simbólico de inicio de sesión de confianza temporal al terminal cliente de destino, de modo que el terminal cliente de destino inicie sesión en el primer servidor y acceda a la página de servicio utilizando el simbólico de inicio de sesión de confianza temporal.

Opcionalmente, el paso de generar una solicitud de adquisición de simbólico en base a la solicitud de acceso y enviar la solicitud de adquisición de simbólico al primer servidor incluye:

adquirir un identificador de inicio de sesión de confianza actual emitido por el primer servidor al segundo servidor, siendo el identificador de inicio de sesión de confianza actual un certificado para adquirir el simbólico de inicio de sesión de confianza temporal; y

escribir el identificador de inicio de sesión de confianza actual en la solicitud de acceso para generar la solicitud de adquisición de simbólico.

Un tercer aspecto de la presente invención proporciona un primer servidor, que incluye:

una unidad de recepción configurada para recibir una solicitud de acceso a la página enviada por un terminal cliente de destino correspondiente a un segundo servidor, utilizándose la solicitud de acceso a la página para solicitar el acceso a una página de servicio proporcionada por el primer servidor;

una unidad de juicio configurada para adquirir un simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página y juzgar si el simbólico de inicio de sesión de confianza temporal tiene un privilegio de servicio para acceder a la página de servicio; y

una unidad de restricción de acceso configurada para permitir que el terminal cliente de destino inicie sesión en el primer servidor de una manera confiable, si el simbólico de inicio de sesión de confianza temporal tiene el privilegio de servicio para acceder a la página de servicio; y devolver la página de servicio que solicita ser accedida mediante el terminal cliente de destino.

Opcionalmente, la unidad de juicio está configurada para:

juzgar si el simbólico de inicio de sesión de confianza temporal y una identificación de servicio de la página de servicio cumplen una primera relación de correspondencia; y

determinar que el simbólico de inicio de sesión de confianza temporal tiene el privilegio de servicio para acceder a la página de servicio, si el simbólico de inicio de sesión de confianza temporal y la identificación de servicio cumplen la primera relación de correspondencia.

Opcionalmente, la unidad de juicio está configurado para:

juzgar si el simbólico de inicio de sesión de confianza temporal y una identificación de servicio de la página de servicio cumplen una primera relación de correspondencia, y juzgar si el simbólico de inicio de sesión de confianza temporal y un identificador de inicio de sesión de confianza actual emitido por el primer servidor al segundo servidor cumplen una segunda relación de correspondencia; y

determinar que el simbólico de inicio de sesión de confianza temporal tiene el privilegio de servicio para acceder a la página de servicio, si el simbólico de inicio de sesión de confianza temporal y la identificación de servicio cumplen la primera relación de correspondencia y el simbólico de inicio de sesión de confianza temporal y el identificador de inicio de sesión de confianza actual cumplen la segunda relación de correspondencia.

Opcionalmente, la unidad de juicio está configurada además para:

antes de juzgar si el simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página tiene un privilegio de servicio para acceder a la página de servicio, juzgar si el simbólico de inicio de sesión de confianza temporal es legal y juzgar si el simbólico de inicio de sesión de confianza temporal expira; y

realizar una operación de juzgar si el simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página tiene un privilegio de servicio para acceder a la página de servicio, si el simbólico de inicio de sesión de confianza temporal es legal y no expira.

Opcionalmente, la página de servicio es una página que se puede cargar al terminal cliente de destino de una manera integrada.

Opcionalmente, la unidad de recepción está configurada además para recibir una solicitud de adquisición de simbólico enviada por el segundo servidor;

la unidad de juicio está configurada además para juzgar, en base a la solicitud de adquisición de simbólico, si el terminal cliente de destino es un terminal cliente de confianza concedida; y

el primer servidor incluye, además:

una unidad de generación configurada para generar el simbólico de inicio de sesión de confianza temporal si el terminal cliente de destino es un terminal cliente de confianza concedida, y establecer un privilegio de servicio de acceso a la página para el simbólico de inicio de sesión de confianza temporal; y

una unidad de envío configurada para enviar el simbólico de inicio de sesión de confianza temporal al terminal cliente de destino utilizando el segundo servidor.

Opcionalmente, la unidad de juicio está configurada además para:

juzgar si la solicitud de adquisición de simbólico incluye el identificador de inicio de sesión de confianza actual emitido por el primer servidor al segundo servidor; y

determinar que el terminal cliente de destino es el terminal cliente de confianza concedida si la solicitud de adquisición de simbólico incluye el identificador de inicio de sesión de confianza actual.

Opcionalmente, la unidad de juicio está configurada además para:

juzgar si existe un primer terminal cliente correspondiente al terminal cliente de destino en el primer servidor; y

determinar que el terminal cliente de destino es el terminal cliente de confianza concedida si existe el primer terminal cliente.

Un cuarto aspecto de la presente invención proporciona un segundo servidor, donde el segundo servidor es un terminal servidor de un terminal cliente de destino e incluye:

un módulo de recepción configurado para recibir una solicitud de inicio de sesión de confianza enviada por el terminal cliente de destino, utilizándose la solicitud de inicio de sesión de confianza para solicitar iniciar sesión en un primer servidor y acceder a una página de servicio proporcionada por el primer servidor; y

un módulo de generación configurado para generar una solicitud de adquisición de simbólico en base a la solicitud de inicio de sesión de confianza y enviar la solicitud de adquisición de simbólico al primer servidor utilizando el módulo de envío; y

el módulo de recepción está configurado además para recibir un simbólico de inicio de sesión de confianza temporal retroalimentado por el primer servidor, teniendo el simbólico de inicio de sesión de confianza temporal un privilegio de servicio para iniciar sesión en el primer servidor y acceder a la página de servicio; y

el módulo de envío está configurado además para enviar el simbólico de inicio de sesión de confianza temporal al terminal cliente de destino, de modo que el terminal cliente de destino inicie sesión en el primer servidor y acceda a la página de servicio utilizando el simbólico de inicio de sesión de confianza temporal.

Opcionalmente, el módulo de generación está configurado para:

adquirir un identificador de inicio de sesión de confianza actual emitido por el primer servidor al segundo servidor, siendo el identificador de inicio de sesión de confianza actual un certificado para adquirir el simbólico de inicio de sesión de confianza temporal; y

escribir el identificador de inicio de sesión de confianza actual en la solicitud de acceso para generar la solicitud de adquisición de simbólico.

Un quinto aspecto de la presente invención proporciona un sistema de inicio de sesión de confianza, que incluye:

un primer servidor;

un segundo servidor; y

un terminal cliente de destino configurado para enviar una solicitud de inicio de sesión de confianza al segundo servidor en respuesta a una operación de usuario en una entrada de acceso de destino, utilizándose la solicitud de inicio de sesión de confianza para solicitar iniciar sesión en el primer servidor y acceder a una página de servicio proporcionada por el primer servidor; recibir un simbólico de inicio de sesión de confianza temporal enviado por el segundo servidor, el simbólico de inicio de sesión de confianza temporal tiene un privilegio de servicio para acceder a la página de servicio; generar, en base al simbólico de inicio de sesión de confianza temporal, una solicitud

de acceso para acceder a la página de servicio y enviar la solicitud de acceso al primer servidor, para solicitar iniciar sesión en el primer servidor y acceder a la página de servicio.

Las una o más soluciones técnicas anteriores en las realizaciones de la presente invención tienen al menos las siguientes soluciones técnicas:

En las realizaciones de la presente invención, cuando se recibe una solicitud de acceso a la página enviada por un terminal cliente de destino correspondiente a un segundo servidor, para solicitar acceso a una página de servicio proporcionada por un primer servidor, se adquiere un simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página y se juzga si el simbólico de inicio de sesión de confianza temporal tiene un privilegio de servicio para acceder a la página de servicio. Si el simbólico de inicio de sesión de confianza temporal tiene el privilegio de servicio, el terminal cliente de destino puede iniciar sesión en el primer servidor de manera confiable y se devuelve la página de servicio a la que el terminal cliente de destino solicita el acceso. De esta manera, un usuario que realiza un inicio de sesión de confianza puede acceder solo a una correspondiente página de servicio bajo una restricción del privilegio de servicio del simbólico de inicio de sesión de confianza temporal, y no puede acceder a otra página de servicio del sistema, resolviendo así un problema de seguridad en un inicio de sesión de confianza en la técnica anterior y mejorando la seguridad del inicio de sesión de confianza.

Breve descripción de los dibujos

La FIG. 1a es un diagrama de flujo de un método de inicio de sesión de confianza en un terminal cliente de destino de acuerdo con la Realización I de la presente solicitud;
la FIG. 1b es un diagrama de flujo de un método de inicio de sesión de confianza en el lado de un segundo servidor de acuerdo con la Realización I de la presente solicitud;
la FIG. 1c es un diagrama de flujo de entrega de simbólico de un método de inicio de sesión de confianza en el lado de un primer servidor de acuerdo con la Realización I de la presente solicitud;
la FIG. 1d es un diagrama de flujo de verificación de simbólico de un método de inicio de sesión de confianza en el lado de un primer servidor de acuerdo con la Realización I de la presente solicitud;
la FIG. 1e es un diagrama de interacción esquemático de un método de inicio de sesión de confianza de acuerdo con la Realización I de la presente solicitud;
la FIG. 2 es un diagrama esquemático de un primer servidor de acuerdo con la Realización II de la presente solicitud;
la FIG. 3 es un diagrama esquemático de un segundo servidor de acuerdo con la Realización II de la presente solicitud; y
la FIG. 4 es un diagrama esquemático de un sistema de inicio de sesión de confianza de acuerdo con la Realización II de la presente solicitud.

Descripción detallada de las realizaciones

El principio principal de implementación, las implementaciones específicas y los correspondientes efectos beneficiosos alcanzables de acuerdo con la solución técnica de las realizaciones de la presente solicitud se describen en detalle a continuación con referencia a los dibujos adjuntos.

Realización I

Esta realización de la presente solicitud proporciona un método de inicio de sesión de confianza, y el método se aplica a un sistema de inicio de sesión de confianza. El sistema incluye dos sistemas de aplicación. Un primer sistema de aplicación incluye un primer servidor y un primer terminal cliente. Un segundo sistema de aplicación incluye un segundo servidor y un segundo terminal cliente (es decir, un terminal cliente de destino). Se proporciona una entrada de acceso de destino a una página de servicio proporcionada por el primer servidor en una interfaz de aplicación del terminal cliente de destino de una manera integrada. Un usuario puede activar, al realizar una operación en la entrada de acceso de destino, el terminal cliente de destino para acceder a la página de servicio proporcionada por el primer servidor por medio del método de inicio de sesión de confianza.

Haciendo referencia a la FIG. 1a, se muestra un método de inicio de sesión de confianza de acuerdo con una realización de la presente solicitud. El método se aplica a un terminal cliente de destino e incluye:

S1.1: Un terminal cliente de destino envía una solicitud de inicio de sesión de confianza a un segundo servidor en respuesta a una operación de usuario en una entrada de acceso de destino, la solicitud de inicio de sesión de confianza se utiliza para solicitar iniciar sesión en un primer servidor y acceder a una página de servicio proporcionada por el primer servidor.

La solicitud de inicio de sesión de confianza incluye una Identificación (ID) de servicio de la página de servicio a ser accedida por el terminal cliente de destino. La ID de servicio se utiliza para indicar una página de servicio específica a ser accedida mediante el terminal cliente de destino. La solicitud de inicio de sesión de confianza incluye además un

número de cuenta de usuario y una contraseña. El número de cuenta de usuario y la contraseña se utilizan para solicitar iniciar sesión en el segundo servidor o permitir que el segundo servidor verifique la legalidad del terminal cliente de destino. Solo cuando el terminal cliente de destino inicia sesión con éxito en el segundo servidor utilizando el número de cuenta de usuario y la contraseña, o solo después de que el terminal cliente de destino pasa la verificación de legalidad realizada por el segundo servidor, el segundo servidor envía un simbólico de inicio de sesión de confianza temporal al terminal cliente de destino en respuesta a la solicitud de inicio de sesión de confianza enviada por el terminal cliente de destino.

S1.2: El terminal cliente de destino recibe el simbólico de inicio de sesión de confianza temporal que se envía por el segundo servidor en respuesta a la solicitud de inicio de sesión de confianza.

El simbólico de inicio de sesión de confianza temporal es un certificado para que el terminal cliente de destino inicie sesión en el primer servidor y acceda a la página de servicio proporcionada por el primer servidor. Un privilegio de servicio para acceder a la página de servicio está escrito en el simbólico de inicio de sesión de confianza temporal. El terminal cliente de destino tiene prohibido acceder a las páginas de servicio más allá del rango del privilegio de servicio del simbólico de inicio de sesión de confianza temporal. El primer servidor genera el simbólico de inicio de sesión de confianza temporal de acuerdo con una solicitud de adquisición de simbólico enviada por el segundo servidor, y se retroalimenta al segundo servidor. Luego, el segundo servidor envía el simbólico de inicio de sesión de confianza temporal al terminal cliente de destino.

S1.3: El terminal cliente de destino genera, en base al simbólico de inicio de sesión de confianza temporal recibido, una solicitud de acceso para acceder a la página de servicio proporcionada por el primer servidor y envía la solicitud de acceso al primer servidor.

En concreto, durante la generación de la solicitud de acceso para acceder a la página de servicio, la solicitud de acceso puede generarse encapsulando el simbólico de inicio de sesión de confianza temporal y la ID de servicio a ser accedida; o también se puede generar encapsulando el simbólico de inicio de sesión de confianza temporal, la ID de servicio a ser accedida y el número de cuenta de usuario. Cuando la solicitud de acceso incluye el número de cuenta de usuario, en base al número de cuenta de usuario en la solicitud de acceso, el primer servidor puede buscar un primer número de cuenta de usuario para el terminal cliente de destino o establecer un primer número de cuenta de usuario en el primer servidor de acuerdo con una relación de correspondencia de usuarios acordada por el primer servidor y el segundo servidor.

Después de S1.3, el terminal cliente de destino espera a que el primer servidor devuelva la página de servicio. Al recibir la página de servicio devuelta por el primer servidor, el terminal cliente de destino realiza una operación en la página de servicio. Debido a que un acceso del terminal cliente de destino a la página de servicio del primer servidor está restringido por el privilegio de servicio del simbólico de inicio de sesión de confianza temporal, el terminal cliente de destino solo puede acceder a una página de servicio dentro del rango del privilegio de servicio del confianza simbólico de inicio de sesión de confianza temporal cuando inicia sesión en el primer servidor de manera confiable, mejorando así la seguridad de acceso a la página de servicio.

Haciendo referencia a la FIG. 1b, se muestra un método de inicio de sesión de confianza de acuerdo con una realización de la presente solicitud. El método se aplica a un segundo servidor e incluye:

S2.1: El segundo servidor recibe una solicitud de inicio de sesión de confianza enviada por un terminal cliente de destino.

S2.2: El segundo servidor genera una solicitud de adquisición de simbólico en base a la solicitud de inicio de sesión de confianza recibida y envía la solicitud de adquisición de simbólico a un primer servidor.

En concreto, la solicitud de adquisición de simbólico se puede generar encapsulando la solicitud de inicio de sesión de confianza y un identificador de servidor del segundo servidor. El primer servidor puede juzgar, de acuerdo con el identificador de servidor, si el segundo servidor es un servidor de confianza concedida. Si el segundo servidor es un servidor de confianza concedida, el primer servidor analiza la solicitud de inicio de sesión de confianza en la solicitud de adquisición de simbólico y retroalimenta un simbólico de inicio de sesión temporal. Si el segundo servidor no es un servidor de confianza, el primer servidor rechaza retroalimentar un simbólico de inicio de sesión temporal al segundo servidor.

La solicitud de adquisición de simbólico puede también generarse encapsulando la solicitud de inicio de sesión de confianza y un identificador de inicio de sesión de confianza actual emitido por el primer servidor al segundo servidor. El identificador de inicio de sesión de confianza actual es un certificado para que el segundo servidor adquiera un simbólico de inicio de sesión de confianza temporal. Si el identificador de inicio de sesión de confianza actual es legal, el primer servidor analiza la solicitud de inicio de sesión de confianza en la solicitud de adquisición de simbólico, para

juzgar si retroalimentar el simbólico de inicio de sesión temporal. Si el identificador de inicio de sesión de confianza actual es ilegal, el primer servidor rechaza enviar el simbólico de inicio de sesión temporal al segundo servidor.

El identificador de inicio de sesión de confianza actual puede ser un número de inicio de sesión de confianza. El primer servidor emite el número de inicio de sesión de confianza al segundo servidor de confianza concedida. El número de inicio de sesión de confianza puede ser un número fijo y es efectivo dentro de un período de concesión de confianza una vez emitido. El número de inicio de sesión de confianza también puede ser un número dinámico actualizado constantemente. El primer servidor actualiza el número de inicio de sesión de confianza de acuerdo con un período de tiempo particular y emite el número de inicio de sesión de confianza actualizado al segundo servidor.

S2.3: El segundo servidor recibe el simbólico de inicio de sesión de confianza temporal retroalimentado por el primer servidor, y envía el simbólico de confianza temporal al terminal cliente de destino.

De forma complementaria, el segundo servidor puede realizar directamente S2.2 después de S2.1. Alternativamente, el segundo servidor puede analizar la solicitud de inicio de sesión de confianza recibida después de S2.1, para juzgar si la solicitud de inicio de sesión de confianza es legal, por ejemplo, para juzgar si el terminal cliente de destino ha iniciado sesión en el segundo servidor o si el primer servidor que proporciona la página de servicio firma un acuerdo con el segundo servidor. Si juzga que la solicitud de inicio de sesión de confianza es legal, el segundo servidor realiza S2.2. Si juzga que la solicitud de inicio de sesión de confianza es ilegal, el segundo servidor devuelve un mensaje de error de solicitud al terminal cliente de destino.

Haciendo referencia a la FIG. 1c, se muestra un método de entrega de simbólico en un método de inicio de sesión de confianza de acuerdo con una realización de la presente solicitud. El método de entrega de simbólico se aplica a un primer servidor e incluye:

S3.1: El primer servidor recibe una solicitud de adquisición de simbólico enviada por un segundo servidor.

El primer servidor puede realizar directamente S3.2 después de recibir la solicitud de adquisición de simbólico; o también puede juzgar, en base a la solicitud de adquisición de simbólico, si un terminal cliente de destino es un terminal cliente de confianza concedida y seleccionar si ejecutar S3.2 de acuerdo con un resultado de juicio.

En base a la solicitud de adquisición de simbólico, el primer servidor puede juzgar, de las siguientes maneras, si el terminal cliente de destino es un terminal cliente de confianza concedida.

En una primera manera, se juzga si la solicitud de adquisición de simbólico incluye un identificador de inicio de sesión de confianza actual emitido por el primer servidor al segundo servidor. Si la solicitud de adquisición de simbólico incluye el identificador de inicio de sesión de confianza actual, se determina que el terminal cliente de destino es un terminal cliente de confianza concedida. De lo contrario, si la solicitud de adquisición de simbólico no incluye el identificador de inicio de sesión de confianza actual, se determina que el terminal cliente de destino no es un terminal cliente de confianza concedida.

En una segunda manera, utilizando una relación de correspondencia de usuario entre el primer servidor y el segundo servidor, se juzga si el terminal cliente de destino es un terminal cliente de confianza concedida. Cuando se establece una relación de inicio de sesión de confianza entre el primer servidor y el segundo servidor, se establece una relación de correspondencia entre usuarios de los dos servidores. Es decir, un usuario objetivo correspondiente a un usuario del segundo servidor se establece o encuentra en el primer servidor. Por ejemplo, al iniciar sesión en el primer servidor, un usuario X del segundo servidor corresponde a un usuario X1 de destino del primer servidor. En consecuencia, el primer servidor puede adquirir un número de cuenta de usuario del terminal cliente de destino en la solicitud de adquisición de simbólico y juzgar si existe un número de cuenta de usuario objetivo correspondiente al número de cuenta de usuario del terminal cliente de destino en el primer servidor. Si existe el número de cuenta de usuario de destino, se determina que el terminal cliente de destino es un terminal cliente de confianza concedida; de lo contrario, se determina que el terminal cliente de destino no es un terminal cliente de confianza concedida.

Al juzgar que el terminal cliente de destino no es un terminal cliente de confianza concedida, el primer servidor devuelve un mensaje de error de solicitud al segundo servidor. Al juzgar que el terminal cliente de destino es un terminal cliente de confianza concedida, el primer servidor continúa ejecutando S3.2.

S3.2: El primer servidor genera un simbólico de inicio de sesión de confianza temporal en base a la solicitud de adquisición de simbólico recibida, y establece un privilegio de servicio de acceso a la página del simbólico de inicio de sesión de confianza temporal.

El privilegio de servicio puede establecerse para una página de servicio particular o múltiples páginas de servicio. El establecimiento de un privilegio de servicio de acceso a la página del simbólico de inicio de sesión de confianza temporal incluye: establecer una primera relación de correspondencia o establecer una primera relación de correspondencia y una segunda relación de correspondencia. La primera relación de correspondencia es una relación de correspondencia entre el simbólico de inicio de sesión de confianza temporal y una ID de servicio de una página de servicio a la que se permite un acceso. La segunda relación de correspondencia es una relación de correspondencia entre el simbólico de inicio de sesión de confianza temporal y un identificador de inicio de sesión de confianza actual emitido por el primer servidor al segundo servidor. Al utilizar la segunda relación de correspondencia, el simbólico de inicio de sesión de confianza temporal está restringido para ser válido y corresponde únicamente a un identificador de inicio de sesión de confianza actual especificado (es decir, corresponde a un servidor especificado). Por lo tanto, se evita que otro servidor usurpe el simbólico de inicio de sesión de confianza temporal. Por ejemplo, en una relación de correspondencia que se muestra en la Tabla 1, un simbólico x1579 de inicio de sesión de confianza temporal es válido únicamente para el segundo servidor Y1 correspondiente a un identificador 4627 de inicio de sesión de confianza actual, y no es válido para otros servidores, por ejemplo, un servidor Y2.

Simbólicos de inicio de sesión de confianza temporales	Segundos servidores	ID de servicio	Identificadores de inicio de sesión de confianza actuales
x1579	Y1	101	4627
y2641	Y2	101	4786
x6478	Y3	103	3451

Tabla 1

En un proceso de generación del simbólico de inicio de sesión de confianza temporal, el simbólico de inicio de sesión de confianza temporal puede generarse de acuerdo con una regla de generación específica para representar legal el simbólico. Alternativamente, se puede establecer un período de validez para cada uno de los simbólicos de inicio de sesión de confianza temporales, y el simbólico de inicio de sesión de confianza temporal deja de ser válido una vez que expira.

S3.3: El primer servidor envía el simbólico de inicio de sesión de confianza temporal generado al terminal cliente de destino utilizando el segundo servidor.

Haciendo referencia a la FIG. 1d, se muestra un método de verificación de simbólico en un método de inicio de sesión de confianza de acuerdo con una realización de la presente solicitud. El método de verificación de simbólico se aplica a un primer servidor e incluye:

S3.4: El primer servidor recibe una solicitud de acceso a la página enviada por un terminal cliente de destino correspondiente a un segundo servidor.

S3.5: El primer servidor adquiere un simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página y juzga si el simbólico de inicio de sesión de confianza temporal tiene un privilegio de servicio para acceder a una página de servicio a la que se solicita acceder mediante el terminal cliente de destino.

En concreto, con el fin de mejorar la eficiencia de la información de retroalimentación del primer servidor, antes del juicio sobre el privilegio del servicio de inicio de sesión de confianza temporal, se puede juzgar en primer lugar si el simbólico de inicio de sesión de confianza temporal es legal o si se expira. Si se juzga que el simbólico de inicio de sesión de confianza temporal es ilegal o expira, se rechaza la solicitud de acceso a la página. Si se considera que el simbólico de inicio de sesión de confianza temporal es legal y no expira, se realiza el juicio en el privilegio de servicio del simbólico de inicio de sesión de confianza temporal.

En un proceso de implementación específica, el privilegio de servicio del simbólico de inicio de sesión de confianza temporal puede juzgarse de cualquiera de las siguientes maneras.

En una primera manera, se juzga si el simbólico de inicio de sesión de confianza temporal y una ID de servicio de una página de servicio a ser accedida mediante un terminal de destino cumplen una primera relación de correspondencia. Específicamente, se puede consultar, de acuerdo con la primera relación de correspondencia entre un simbólico de inicio de sesión de confianza temporal y una ID de servicio que se establece mediante el primer servidor, si el simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página corresponde a una ID de servicio en solicitud de acceso. Si el resultado de una consulta indica que se corresponden entre sí, se considera que el simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página coincide con la ID de servicio, y el simbólico de inicio de sesión de confianza temporal tiene el privilegio de servicio para acceder a una correspondiente

página de servicio; de lo contrario, el simbólico de inicio de sesión de confianza temporal no tiene el privilegio de servicio para acceder a la correspondiente página de servicio.

En una segunda manera, se juzga si el simbólico de inicio de sesión de confianza temporal y una ID de servicio de una página de servicio a ser accedida mediante un terminal de destino cumplen una primera relación de correspondencia, y se juzga si el simbólico de inicio de sesión de confianza temporal y un identificador de inicio de sesión de confianza actual cumplen una segunda relación de correspondencia, el primer servidor emite el identificador de inicio de sesión de confianza actual a un segundo servidor al que pertenece el terminal cliente de destino. Cuando se juzga que el simbólico de inicio de sesión de confianza temporal y la ID de servicio de la página de servicio a ser accedida mediante el terminal de destino cumplen la primera relación de correspondencia, y que el simbólico de inicio de sesión de confianza temporal y el identificador de inicio de sesión de confianza actual cumplen la segunda relación de correspondencia, el identificador de inicio de sesión de confianza actual se emite por el primer servidor a un segundo servidor al que pertenece el terminal cliente de destino, el simbólico de inicio de sesión de confianza temporal tiene el privilegio de servicio para acceder a una correspondiente página de servicio. De lo contrario, el simbólico de inicio de sesión de confianza temporal no tiene el privilegio de servicio para acceder a la correspondiente página de servicio. Por ejemplo, se supone que en la Tabla 1 se muestra una relación de correspondencia establecida en el primer servidor para el simbólico de inicio de sesión de confianza temporal, el simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página recibida por el primer servidor es x6478, la ID de servicio a ser accedida es 103, y el identificador de inicio de sesión de confianza actual del segundo servidor al que pertenece el terminal cliente de destino es 3450. El primer servidor juzga, de acuerdo con la Tabla 1, que el simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página y la ID de servicio cumplen la primera relación de correspondencia, pero el simbólico de inicio de sesión de confianza temporal y el identificador de inicio de sesión de confianza actual no cumplen la segunda relación de correspondencia (el simbólico x6478 de inicio de sesión de confianza temporal corresponde a un identificador 3451 de inicio de sesión de confianza actual, en lugar de 3450). El simbólico x6478 de inicio de sesión de confianza temporal es un simbólico ilegal que puede ser usurpado o expirado. Por lo tanto, el primer servidor puede rechazar la solicitud de acceso al servicio actual.

S3.6: Si se juzga que el simbólico de inicio de sesión de confianza temporal tiene el privilegio de servicio para acceder a correspondiente la página de servicio, el primer servidor permite que el terminal cliente de destino inicie sesión en el primer servidor de manera confiable y devuelve la página de servicio a la que se solicita acceder mediante el terminal cliente de destino. De lo contrario, si se juzga que el simbólico de inicio de sesión de confianza temporal no tiene el privilegio de servicio para acceder a la correspondiente página de servicio, el primer servidor prohíbe al terminal cliente de destino acceder a la correspondiente página de servicio.

En un proceso de implementación específica, el primer servidor permite al terminal cliente de destino iniciar sesión en el primer servidor de una manera confiable. El terminal cliente de destino puede implementar un inicio de sesión de confianza solo en el primer servidor y no redirige a un primer terminal cliente del primer servidor. En cambio, la página de servicio se devuelve al terminal cliente de destino, mejorando así la experiencia de usuario. Por ejemplo, para un sistema A de APP de mapas y un sistema B de APP de pago, un usuario del sistema A de APP de mapas hace clic en una entrada de acceso en el terminal cliente de destino (es decir, software de terminal cliente de mapas), para solicitar el acceso a una página C de servicio del sistema B de APP de pago. El sistema B de APP de pago solo necesita verificar y completar un inicio de sesión de confianza de un usuario del terminal cliente de destino en el sistema B, y luego devolver la página C de servicio al software del terminal cliente de mapas, sin la necesidad de redirigir al software de terminal cliente de pago del sistema B de APP de pago.

Además, la página de servicio proporcionada por el primer servidor puede ser una página que se carga al terminal cliente de destino de una manera integrada. Un proceso de servicio y una presentación de servicio de la página de servicio se implementan utilizando una página H5 (es decir, una página html5, que es una página implementada utilizando el quinto lenguaje revisado del lenguaje de marcado de hipertexto), reduciendo así el desarrollo de un primer sistema de aplicación del primer servidor. El primer servidor solo necesita completar el inicio de sesión de confianza y devolver la página, logrando así el objetivo de promocionar la página de servicio a más sistemas de aplicación y terminales cliente.

Después del inicio de sesión de confianza, el primer servidor puede enterrar un identificador en una correspondiente página de servicio. Por ejemplo, un control sobre una sesión entre el terminal cliente de destino y la página de servicio se escribe de acuerdo con un resultado de inicio de sesión de confianza, y un identificador de un usuario del terminal cliente de destino se escribe en la sesión, para indicar el éxito del inicio sesión de confianza. El terminal cliente de destino no necesita iniciar sesión en el primer servidor nuevamente dentro de un período de validez. La página de servicio puede responder directamente a una operación de servicio del terminal cliente de destino dentro del período de validez.

Haciendo referencia a la FIG. 1e, a continuación, se describe completamente el método de inicio de sesión de confianza de acuerdo con una realización de la presente solicitud utilizando una instancia de interacción.

S1.1: Un terminal cliente de destino envía una solicitud de inicio de sesión de confianza a un segundo servidor en respuesta a una operación de usuario en una entrada de acceso de destino.

Por ejemplo, se supone que una entrada de acceso de seguro de automóvil de una APP de pago está embebida en una APP de mapa. Un usuario B del terminal cliente de destino hace clic en la entrada de acceso de seguro de automóvil en la APP de mapa. El terminal cliente de destino envía una solicitud de inicio de sesión de confianza a un segundo servidor de la APP de mapas en respuesta a la operación de toque. Una ID de servicio de una página de servicio a ser accedida y un número de cuenta de usuario del terminal cliente de destino se escriben en la solicitud de inicio de sesión de confianza.

S2.1: El segundo servidor recibe la solicitud de inicio de sesión de confianza enviada por el terminal cliente de destino.

S2.2: El segundo servidor genera una solicitud de adquisición de simbólico en base a la solicitud de inicio de sesión de confianza recibida, y envía la solicitud de adquisición de simbólico a un primer servidor.

El segundo servidor puede encapsular la solicitud de inicio de sesión de confianza y un identificador de inicio de sesión de confianza actual emitido por el primer servidor para generar la solicitud de adquisición de simbólico, y luego enviar la solicitud de adquisición simbólico generada después de la encapsulación al primer servidor. Por ejemplo, el segundo servidor de la APP de mapa puede encapsular un identificador XXX de inicio de sesión de confianza actual emitido por un servidor de la APP de pago y la solicitud de inicio de sesión de confianza recibida, y luego enviar una solicitud de adquisición de simbólico generada después de la encapsulación al primer servidor de la APP de pago.

S3.1: El primer servidor recibe la solicitud de adquisición de simbólico enviada por el segundo servidor.

S3.2: El primer servidor genera un simbólico de inicio de sesión de confianza temporal y establece un privilegio de servicio de acceso a la página del simbólico de inicio de sesión de confianza temporal.

Por ejemplo, el primer servidor de la APP de pago adquiere un identificador de inicio de sesión de confianza actual de la solicitud de adquisición de simbólico recibida; y determina si el identificador de inicio de sesión de confianza actual es consistente con un identificador de inicio de sesión de confianza actual guardado en el primer servidor y emitido al segundo servidor. Si son consistentes, el primer servidor puede determinar el privilegio de servicio de acceso a la página del terminal cliente de destino de acuerdo con la solicitud de adquisición de simbólico. Si son inconsistentes, el primer servidor rechaza la solicitud de adquisición de simbólico. Si se determina que el terminal cliente de destino de la APP de mapas puede acceder únicamente a una página de seguro de automóvil de la APP de pago, se genera el simbólico de inicio de sesión de confianza temporal y se establece un privilegio de servicio de acceso a la página del simbólico de inicio de sesión de confianza temporal que solo puede acceder a la página de seguro de automóvil. Luego, el simbólico de inicio de sesión de confianza temporal generado se envía al segundo servidor de la APP de mapas.

S3.3: El primer servidor envía el simbólico de inicio de sesión de confianza temporal generado al terminal cliente de destino utilizando el segundo servidor.

En concreto, el primer servidor retroalimenta en primer lugar el simbólico de inicio de sesión de confianza temporal al segundo servidor como información de retroalimentación de la solicitud de adquisición de simbólico. Luego, el segundo servidor envía el simbólico de inicio de sesión de confianza temporal al terminal cliente de destino.

S2.3: El segundo servidor recibe el simbólico de inicio de sesión de confianza temporal retroalimentado por el primer servidor, y envía el simbólico de inicio de sesión de confianza temporal al terminal cliente de destino. En concreto, el segundo servidor también puede enviar el identificador de inicio de sesión de confianza actual emitido por el primer servidor y el simbólico de inicio de sesión de confianza temporal juntos al terminal cliente de destino.

S1.2: El terminal cliente de destino recibe el simbólico de inicio de sesión de confianza temporal enviado por el segundo servidor.

S1.3: El terminal cliente de destino genera, en base al simbólico de inicio de sesión de confianza temporal recibido, una solicitud de acceso a la página para acceder a la página de servicio, y envía la solicitud de acceso a la página al primer servidor, para solicitar iniciar sesión en el primer servidor y acceder a la página de servicio proporcionada por el primer servidor.

Por ejemplo, el terminal cliente de destino puede encapsular información, tal como el simbólico de inicio de sesión de confianza temporal recibido, la ID de servicio a ser accedida y el identificador de inicio de sesión de confianza temporal, y enviar la solicitud de acceso a la página generada después de la encapsulación al primer servidor de la APP de pago.

S3.4: El primer servidor recibe la solicitud de acceso a la página enviada por el terminal cliente de destino correspondiente al segundo servidor.

S3.5: El primer servidor adquiere el simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página y juzga si el simbólico de inicio de sesión de confianza temporal tiene un privilegio de servicio para acceder a la página de servicio que solicita ser accedida mediante el terminal cliente de destino.

Por ejemplo, se supone que la solicitud de acceso de página incluye el simbólico de inicio de sesión de confianza temporal, la ID de servicio a ser accedida, y el identificador de inicio de sesión de confianza actual. De acuerdo con una tabla de relación de correspondencia que se muestra como Tabla 1 y establecida para el simbólico de inicio de sesión de confianza temporal de antemano, el primer servidor de la APP de pago puede juzgar si el simbólico de inicio de sesión de confianza temporal y la ID de servicio cumplen una primera relación de correspondencia, y juzgar si el simbólico de inicio de sesión de confianza temporal y el identificador de inicio de sesión de confianza actual cumplen una segunda relación de correspondencia. Al juzgar que el simbólico de inicio de sesión de confianza temporal y la ID de servicio cumplen la primera relación de correspondencia, y que el simbólico de inicio de sesión de confianza temporal y el identificador de inicio de sesión de confianza actual cumplen la segunda relación de correspondencia, se determina que el simbólico de inicio de sesión de confianza temporal tiene el privilegio de servicio para acceder a la página de servicio que solicita ser accedida mediante el terminal cliente de destino. De lo contrario, se determina que el simbólico de inicio de sesión de confianza temporal no tiene el privilegio de servicio para acceder a la página de servicio que solicita ser accedida mediante el terminal cliente de destino, y se rechaza la solicitud de acceso a la página.

S3.6: Si se juzga que el simbólico de inicio de sesión de confianza temporal tiene el privilegio de servicio para acceder a la correspondiente página de servicio, el primer servidor permite que el terminal cliente de destino inicie sesión en el primer servidor de manera confiable y devuelve la página de servicio que solicita ser accedida mediante el terminal cliente de destino.

En la realización anterior, emitiendo un simbólico de inicio de sesión de confianza temporal, un primer servidor restringe un privilegio de un terminal cliente de destino de un segundo servidor para acceder a una página de servicio después de que el terminal cliente de destino complete un inicio de sesión de confianza, protegiendo así eficazmente otras páginas de servicio en el primer servidor, resolviendo un problema de seguridad en una solución de inicio de sesión de confianza aplicada universalmente en la técnica anterior y mejorando la seguridad del inicio de sesión de confianza. Además, la presente solicitud utiliza una manera de devolver la página de servicio, de modo que se puede implementar un inicio de sesión complicado desde un segundo sistema de aplicación a un primer sistema de aplicación y luego de vuelta al segundo sistema de aplicación. De esta forma, se evita un redireccionamiento repetido entre sistemas de aplicación y se mejora la experiencia de usuario.

Realización II

En base a un mismo concepto de la invención, una realización de la presente solicitud proporciona además en consecuencia un primer servidor 200. Como se muestra en la FIG. 2, el primer servidor 200 incluye:

una unidad 21 de recepción configurada para recibir una solicitud de acceso a una página enviada por un terminal cliente de destino correspondiente a un segundo servidor, utilizándose la solicitud de acceso a la página para solicitar acceder a una página de servicio proporcionada por el primer servidor;

una unidad 22 de juicio configurada para adquirir un simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página y juzgar si el simbólico de inicio de sesión de confianza temporal tiene un privilegio de servicio para acceder a la página de servicio; y

una unidad 23 de restricción de acceso configurada para permitir que el terminal cliente de destino inicie sesión en el primer servidor de manera confiable, si el simbólico de inicio de sesión de confianza temporal tiene el privilegio de servicio para acceder a la página de servicio y devolver la página de servicio que solicita ser accedida mediante el terminal cliente de destino.

La página de servicio es una página que se puede cargar al terminal cliente de destino de una manera integrada.

Como una implementación adicional, la unidad 22 de juicio puede estar configurada para: juzgar si el simbólico de inicio de sesión de confianza temporal y una identificación de servicio de la página de servicio cumplen una primera relación de correspondencia; y determinar que el simbólico de inicio de sesión de confianza temporal tiene el privilegio

de servicio para acceder a la página de servicio, si el simbólico de inicio de sesión de confianza temporal y la identificación de servicio cumplen la primera relación de correspondencia, o de lo contrario, determinar que el simbólico de inicio de sesión de confianza temporal no tiene el privilegio de servicio.

La unidad 22 de juicio puede estar configurada además para: juzgar si el simbólico de inicio de sesión de confianza temporal y una identificación de servicio de la página de servicio cumplen una primera relación de correspondencia, y juzgar si el simbólico de inicio de sesión de confianza temporal y un identificador de inicio de sesión de confianza actual emitido por el primer servidor al segundo servidor cumplen una segunda relación de correspondencia; y determinar que el simbólico de inicio de sesión de confianza temporal tiene el privilegio de servicio para acceder a la página de servicio, si el simbólico de inicio de sesión de confianza temporal y la identificación de servicio cumplen la primera relación de correspondencia y el simbólico de inicio de sesión de confianza temporal y el identificador de inicio de sesión de confianza actual cumplen la segunda relación de correspondencia.

Antes de juzgar si el simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página tiene un privilegio servicio para acceder a la página de servicio, la unidad 22 de juicio puede estar configurada además para: juzgar si el simbólico de inicio de sesión de confianza temporal es legal, y juzgar si el simbólico de inicio de sesión de confianza temporal expira; y realizar una operación de juzgar si el simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página tiene un privilegio de servicio para acceder a la página de servicio, si el simbólico de inicio de sesión de confianza temporal es legal y no expira.

Como una implementación opcional, la unidad 21 de recepción puede estar configurada además para recibir una solicitud de adquisición de simbólico enviada por el segundo servidor. La unidad 22 de juicio puede estar configurada además para juzgar, en base a la solicitud de adquisición de simbólico, si el terminal cliente de destino es un terminal cliente de confianza concedida. En consecuencia, el primer servidor 200 incluye además: una unidad 24 de generación configurada para generar el simbólico de inicio de sesión de confianza temporal si el terminal cliente de destino es un terminal cliente de confianza concedida, y establecer un privilegio de servicio de acceso a la página para el simbólico de inicio de sesión de confianza temporal; y una unidad 25 de envío configurada para enviar el simbólico de inicio de sesión de confianza temporal al terminal cliente de destino utilizando el segundo servidor.

Como una implementación opcional, la unidad 22 de juicio puede estar configurada además para: juzgar si la solicitud de adquisición de simbólico incluye el identificador de inicio de sesión de confianza actual emitido por el primer servidor al segundo servidor, y determinar que el terminal cliente de destino es el terminal cliente de confianza concedida si la solicitud de adquisición de simbólico incluye el identificador de inicio de sesión de confianza actual; o juzgar si existe un primer terminal cliente correspondiente al terminal cliente de destino en el primer servidor, y determinar que el terminal cliente de destino es el terminal cliente de confianza concedida si existe el primer terminal cliente.

Del mismo modo, una realización de la presente solicitud proporciona además un segundo servidor 300, siendo el segundo servidor un terminal servidor de un terminal cliente de destino. Como se muestra en la FIG. 3, el segundo servidor 300 incluye:

un módulo 31 de recepción configurado para recibir una solicitud de inicio de sesión de confianza enviada por el terminal cliente de destino, utilizándose la solicitud de inicio de sesión de confianza para solicitar iniciar sesión en un primer servidor y acceder a una página de servicio proporcionada por el primer servidor; y

un módulo 32 de generación configurado para generar una solicitud de adquisición de simbólico en base a la solicitud de inicio de sesión de confianza, y enviar la solicitud de adquisición de simbólico al primer servidor utilizando el módulo 33 de envío; dónde

el módulo 31 de recepción está configurado además para recibir un simbólico de inicio de sesión de confianza temporal retroalimentado por el primer servidor, teniendo el simbólico de inicio de sesión de confianza temporal un privilegio de servicio para iniciar sesión en el primer servidor y acceder a la página de servicio; y

el módulo 33 de envío está configurado además para retroalimentar el simbólico de inicio de sesión de confianza temporal al terminal cliente de destino, de modo que el terminal cliente de destino inicie sesión en el primer servidor y acceda a la página de servicio utilizando el simbólico de inicio de sesión de confianza temporal.

Específicamente, el módulo 32 de generación está configurado para adquirir un identificador de inicio de sesión de confianza actual emitido por el primer servidor al segundo servidor, siendo el identificador de inicio de sesión de confianza actual un certificado para la adquisición de el simbólico de inicio de sesión de confianza temporal; y escribir el identificador de inicio de sesión de confianza actual en la solicitud de acceso para generar la solicitud de adquisición de simbólico.

En base al método de inicio de sesión de confianza proporcionado por la realización anterior, una realización de la presente solicitud proporciona además en consecuencia un sistema de inicio de sesión de confianza. Como se muestra en la FIG. 4, el sistema incluye:

un primer servidor 200;

un segundo servidor 300; y

un terminal 100 cliente de destino configurado para enviar una solicitud de inicio de sesión de confianza al segundo servidor 300 en respuesta a una operación de usuario en una entrada de acceso de destino, utilizándose la solicitud de inicio de sesión de confianza para solicitar iniciar sesión en el primer servidor 200 y acceder a una página de servicio proporcionada por el primer servidor 200; recibir un simbólico de inicio de sesión de confianza temporal enviado por el segundo servidor 300, teniendo el simbólico de inicio de sesión de confianza temporal un privilegio de servicio para acceder a la página de servicio; generar, en base al simbólico de inicio de sesión de confianza temporal, una solicitud de acceso para acceder a la página de servicio y enviar la solicitud de acceso al primer servidor 200, para solicitar iniciar sesión en el primer servidor 200 y acceder a la página de servicio.

Las maneras específicas en las que los módulos y las unidades del aparato en la realización anterior realizan operaciones, se han descrito en detalle en la realización del método relacionado, por lo que los detalles no se describen de nuevo en el presente documento.

Debe entenderse que, la presente invención no está limitada a la estructura precisa descrita anteriormente y mostrada en los dibujos adjuntos, y se pueden hacer diversas modificaciones y cambios sin apartarse del alcance de la presente invención. El alcance de la presente invención está limitado únicamente por las reivindicaciones adjuntas.

Las realizaciones anteriores simplemente describen realizaciones preferidas de la presente invención, pero no pretenden limitar la presente invención.

Las realizaciones de la materia objeto y las operaciones descritas en esta memoria descriptiva se pueden implementar en circuitos electrónicos digitales, o en software, firmware o hardware de computadora, incluidas las estructuras dadas a conocer en esta memoria descriptiva y sus equivalentes estructurales, o en combinaciones de una o más de ellas. Las realizaciones de la materia objeto descrito en esta memoria descriptiva se pueden implementar como uno o más programas informáticos, es decir, uno o más módulos de instrucciones de programa informático, codificados en medios de almacenamiento de computadora no transitorios para su ejecución o para controlar la operación de, aparatos de procesamiento de datos. Alternativa o adicionalmente, las instrucciones del programa se pueden codificar en una señal propagada generada artificialmente, por ejemplo, una señal eléctrica, óptica o electromagnética generada por una máquina, que se genera para codificar información para su transmisión a un aparato de recepción adecuado para su ejecución por un aparato de procesamiento de datos. Un medio de almacenamiento de computadora puede ser, o estar incluido en, un dispositivo de almacenamiento legible por computadora, un sustrato de almacenamiento legible por computadora, una matriz o dispositivo de memoria de acceso aleatorio o en serie, o una combinación de uno o más de ellos. Además, aunque un medio de almacenamiento de computadora no es una señal propagada, un medio de almacenamiento de computadora puede ser un origen o destino de instrucciones de programa informático codificadas en una señal propagada generada artificialmente. El medio de almacenamiento de computadora también puede ser, o estar incluido en, uno o más componentes o medios físicos separados (por ejemplo, múltiples discos compactos (CD), discos de vídeo digital (DVD), discos magnéticos u otros dispositivos de almacenamiento).

Las operaciones descritas en esta memoria descriptiva pueden implementarse como operaciones realizadas por un aparato de procesamiento de datos sobre los datos almacenados en uno o más dispositivos de almacenamiento legibles por computada o recibidos de otros orígenes.

El término “tiempo-real”, “tiempo real”, “tiempo real (rápido) (RFT)”, “tiempo real casi real (NRT)”, “tiempo cuasi real” o términos similares (como los entenderá un experto en la técnica), significa que una acción y una respuesta son temporalmente próximas de manera que un individuo percibe que la acción y la respuesta ocurren sustancialmente de manera simultánea. Por ejemplo, la diferencia de tiempo para que se muestre una respuesta (o para el inicio de una pantalla) de datos después de la acción del individuo para acceder a los datos puede ser menos de 1 milisegundo (ms), menos de 1 segundo (s) o menos de 5 s. Si bien los datos solicitados no necesitan mostrarse (o iniciarse para mostrar) instantáneamente, se muestran (o inician para mostrar) sin un retraso intencional, teniendo en cuenta las limitaciones de procesamiento de un sistema informático descrito y el tiempo requerido para, por ejemplo, recopilar, medir, analizar, procesar, almacenar o transmitir con precisión los datos.

Los términos “aparato de procesamiento de datos”, “computadora”, o “dispositivo informático” abarcan todos los tipos de aparatos, dispositivos y máquinas para el procesamiento de datos, incluyendo a modo de ejemplo, un procesador programable, un ordenador, un sistema en chip, o múltiples, o combinaciones, de los anteriores. El aparato puede incluir circuitos lógicos de propósito especial, por ejemplo, una unidad central de procesamiento (CPU), una matriz de compuertas programables en campo (FPGA) o un circuito integrado de aplicación específica (ASIC). El aparato también puede incluir, además del hardware, código que crea un entorno de ejecución para el programa informático en cuestión, por ejemplo, código que constituye el firmware del procesador, una pila de protocolos, un sistema de gestión de bases de datos, un sistema operativo (por ejemplo, LINUX, UNIX, WINDOWS, MAC OS, ANDROID, IOS, otro sistema operativo o una combinación de sistemas operativos), un entorno de ejecución multiplataforma, una

máquina virtual o una combinación de uno o más de ellos. El aparato y el entorno de ejecución pueden realizar diversas infraestructuras de modelos informáticos diferentes, tales como servicios web, informática distribuida e infraestructuras informáticas en malla.

Un programa informático (también conocido como programa, software, aplicación de software, módulo de software, unidad de software, script o código) se puede escribir en cualquier forma de lenguaje de programación, incluidos los lenguajes compilados o interpretados, los lenguajes declarativos o procedimentales, y se puede implementar de cualquier forma, incluso como programa autónomo o como un módulo, componente, subrutina, objeto u otra unidad adecuada para su uso en un entorno informático. Un programa informático puede, pero no es necesario, corresponder a un archivo en un sistema de archivos. Un programa se puede almacenar en una porción de un archivo que contiene otros programas o datos (por ejemplo, uno o más scripts almacenados en un documento de lenguaje de marcado), en un solo archivo dedicado al programa en cuestión o en múltiples archivos coordinados (por ejemplo, archivos que almacenan uno o más módulos, subprogramas o porciones de código). Un programa informático se puede desplegar para que se ejecute en una computadora o en múltiples computadoras que están ubicadas en un sitio o distribuidas en múltiples sitios e interconectadas por una red de comunicaciones.

Los procesadores adecuados para la ejecución de un programa informático incluyen, a modo de ejemplo, microprocesadores tanto de uso general como especial, y uno o más procesadores de cualquier tipo de computadora digital. Generalmente, un procesador recibirá instrucciones y datos desde una memoria de solo lectura o una memoria de acceso aleatorio o ambas. Los elementos esenciales de una computadora son un procesador para realizar acciones de acuerdo con las instrucciones y uno o más dispositivos de memoria para almacenar instrucciones y datos. Generalmente, un ordenador también incluirá, o estará operativamente acoplado para recibir datos o transferir datos a, o ambos, uno o más dispositivos de almacenamiento masivo para almacenar datos, por ejemplo, discos magnéticos, magneto-ópticos o discos ópticos. Sin embargo, una computadora no necesita tener tales dispositivos. Además, una computadora puede integrarse en otro dispositivo, por ejemplo, un dispositivo móvil, un asistente digital personal (PDA), una consola de juegos, un receptor del sistema de posicionamiento global (GPS) o un dispositivo de almacenamiento portátil (por ejemplo, una unidad flash universal de bus serie (USB)), por nombrar solo algunos. Los dispositivos adecuados para almacenar instrucciones y datos de programa informático incluyen todas las formas de memoria, medios y dispositivos de memoria no volátiles, incluidos, a modo de ejemplo, dispositivos de memoria semiconductores, por ejemplo, memoria de solo lectura programable borrable (EPROM), memoria de solo lectura programable borrable eléctricamente (EEPROM) y dispositivos de memoria flash; discos magnéticos, por ejemplo, discos duros internos o discos extraíbles; discos magneto-ópticos; y discos CD-ROM y DVD-ROM. El procesador y la memoria pueden complementarse o incorporarse en circuitos lógicos de propósito especial.

Los dispositivos móviles pueden incluir teléfonos móviles (por ejemplo, teléfonos inteligentes), tabletas, dispositivos ponibles (por ejemplo, relojes inteligentes, gafas inteligentes, tela inteligente, joyería inteligente), dispositivos implantados dentro del cuerpo humano (por ejemplo, biosensores, marcapasos inteligentes, implantes cocleares) u otros tipos de dispositivos móviles. Los dispositivos móviles pueden comunicarse de forma inalámbrica (por ejemplo, utilizando señales de radiofrecuencia (RF)) con diversas redes de comunicaciones (descritas a continuación). Los dispositivos móviles pueden incluir sensores para determinar características del entorno actual del dispositivo móvil. Los sensores pueden incluir cámaras, micrófonos, sensores de proximidad, sensores GPS, sensores de movimiento, acelerómetros, sensores de luz ambiental, sensores de humedad, giroscopios, brújulas, barómetros, sensores de huellas dactilares, sistemas de reconocimiento facial, sensores de RF (por ejemplo, radios Wi-Fi y móviles), sensores térmicos u otros tipos de sensores. Por ejemplo, las cámaras pueden incluir una cámara orientada hacia adelante o hacia atrás con lentes fijas o móviles, un flash, un sensor de imagen y un procesador de imagen. La cámara puede ser una cámara de megapíxeles capaz de capturar detalles para reconocimiento facial y/o de iris. La cámara junto con un procesador de datos y la información de autenticación almacenada en la memoria o al que se accede de forma remota pueden formar un sistema de reconocimiento facial. El sistema de reconocimiento facial o uno o más sensores, por ejemplo, micrófonos, sensores de movimiento, acelerómetros, sensores GPS o sensores de RF, se pueden utilizar para la autenticación del usuario

Para proporcionar para la interacción con un usuario, las realizaciones de la materia objeto descrita en esta memoria descriptiva se pueden implementar en una computadora que tiene un dispositivo de visualización y un dispositivo de entrada, por ejemplo, una pantalla de cristal líquido (LCD) o pantalla de diodo orgánico emisor de luz (OLED)/realidad virtual (VR)/realidad aumentada (AR) para mostrar información al usuario y una pantalla táctil, teclado y un dispositivo señalador, por ejemplo, un ratón o una bola de seguimiento, mediante el cual el usuario puede proporcionar información a la computadora. También se pueden utilizar otros tipos de dispositivos para permitir la interacción con un usuario; por ejemplo, la retroalimentación proporcionada al usuario puede ser cualquier forma de retroalimentación sensorial, por ejemplo, retroalimentación visual, retroalimentación auditiva o retroalimentación táctil; y la entrada del usuario se puede recibir de cualquier forma, incluida la entrada acústica, de voz o táctil. Además, una computadora puede interactuar con un usuario enviando documentos y recibiendo documentos desde un dispositivo que se utiliza

por el usuario; por ejemplo, enviando páginas web a un navegador web en el dispositivo cliente de un usuario en respuesta a solicitudes recibidas desde el navegador web.

Las realizaciones de la materia objeto descrita en esta memoria descriptiva se pueden implementar utilizando dispositivos informáticos interconectados por cualquier forma o medio de comunicación de datos digital inalámbrica o cableada (o combinación de los mismos), por ejemplo, una red de comunicaciones. Ejemplos de redes de comunicaciones incluyen una red de área local (LAN), una red de acceso por radio (RAN), una red de área metropolitana (MAN) y una red de área amplia (WAN). La red de comunicaciones puede incluir todo o una porción del Internet, otra red de comunicaciones o una combinación de redes de comunicaciones. La información se puede transmitir en la red de comunicaciones de acuerdo con diversos protocolos y estándares, incluidos los protocolos interoperabilidad mundial para el acceso por microondas (WIMAX), evolución a largo plazo (LTE), acceso múltiple por división de código (CDMA), 5G, IEEE 802.11 a/b/g/n o protocolos 802.20 (o una combinación de 802.11xy 802.20 u otros protocolos consistentes con la presente divulgación), Protocolo de Internet (IP), retransmisión de tramas, modo de transferencia asíncrona (ATM), ETHERNET u otros protocolos o combinaciones de protocolos. La red de comunicaciones puede transmitir voz, video, datos biométricos o de autenticación, u otra información entre los dispositivos informáticos conectados.

Las realizaciones de la materia objeto descrita en esta memoria descriptiva se pueden implementar utilizando clientes y servidores interconectados mediante una red de comunicaciones. Por lo general, un cliente y un servidor son remotos entre sí y normalmente interactúan a través de una red de comunicaciones. La relación de cliente y servidor surge en virtud de programas informáticos que se ejecutan en las respectivas computadoras y tienen una relación cliente-servidor entre sí. Un cliente, por ejemplo, un dispositivo móvil, puede realizar transacciones por sí mismo, con un servidor, o a través de un servidor, por ejemplo, realizando transacciones de compra, venta, pago, entrega, envío o préstamo, o autorizando las mismas.

Aunque esta memoria descriptiva contiene muchos detalles de implementación específicos, estos no deben interpretarse como limitaciones en el alcance de la divulgación y lo que se reivindica. Ciertas características que se describen en esta memoria descriptiva en el contexto de implementaciones separadas también pueden implementarse, en combinación, en una sola implementación. A la inversa, diversas características que se describen en el contexto de una única implementación también se pueden implementar en múltiples implementaciones, por separado o en cualquier subcombinación adecuada. Si bien las operaciones se describen y reivindican en un orden particular, esto no debe entenderse como que requiere que dichas operaciones se realicen en el orden particular mostrado o en orden secuencial, o que se realicen todas las operaciones ilustradas (algunas operaciones pueden considerarse opcionales). Según corresponda, se puede realizar procesamiento multitarea o en paralelo (o una combinación de procesamiento multitarea y en paralelo).

REIVINDICACIONES

1. Un método de inicio de sesión de confianza implementado por computadora aplicado a un sistema de inicio de sesión de confianza que comprende un primer sistema de aplicación que incluye un primer servidor y un primer terminal cliente y un segundo sistema de aplicación que incluye un segundo servidor y un terminal cliente de destino, que comprende:

emitir, desde el primer servidor y al segundo servidor, un identificador de inicio de sesión de confianza actual que certifica al segundo servidor para obtener un simbólico de inicio de sesión de confianza temporal;

recibir, en el primer servidor y desde el segundo servidor, una solicitud de adquisición de simbólico de inicio de sesión de confianza (S3.1), basándose la solicitud de adquisición de simbólico de inicio de sesión de confianza en una solicitud de inicio de sesión de confianza que i) especifica una solicitud de acceso a la página de servicio que comprende una solicitud para acceder a una página de servicio proporcionada por el primer servidor, y ii) fue enviada al segundo servidor por el terminal cliente de destino, y

el identificador de inicio de sesión de confianza actual; generar, mediante el primer servidor, un simbólico de inicio de sesión de confianza temporal en base a la solicitud de adquisición de simbólico recibida y establecer un permiso de servicio de acceso a la página de servicio del simbólico de inicio de sesión de confianza temporal (S3.2);

determinar, mediante el primer servidor, si el identificador de inicio de sesión de confianza actual es legal o no;

en respuesta a determinar que el identificador de inicio de sesión de confianza actual es legal, enviar, desde el primer servidor, el simbólico de inicio de sesión de confianza temporal al segundo servidor, en donde el segundo servidor envía el simbólico de inicio de sesión de confianza temporal al terminal cliente de destino (S3.3);

recibir, en el primer servidor y desde el terminal cliente de destino, la solicitud de acceso a la página de servicio (S3.4), en donde la solicitud de acceso a la página de servicio incluye el simbólico de inicio de sesión de confianza temporal;

obtener, mediante el primer servidor y a partir de la solicitud de acceso a la página de servicio recibida, el simbólico de inicio de sesión de confianza temporal y determinar si el simbólico de inicio de sesión de confianza temporal tiene permiso de servicio para acceder a la página de servicio solicitada para ser accedida por el terminal cliente de destino (S3.5);

si se determina que el simbólico de inicio de sesión de confianza temporal tiene permiso de servicio para acceder a la correspondiente página de servicio, permitir, mediante el primer servidor, el inicio de sesión de confianza del terminal cliente de destino en el primer servidor y devolver, desde el primer servidor y al cliente de destino terminal, la página de servicio solicitada para ser accedida por el terminal cliente de destino (S3.6).

2. El método de la reivindicación 1, en donde determinar si el simbólico de inicio de sesión de confianza temporal tiene permiso de servicio para acceder a la página de servicio solicitada comprende:

determinar si el simbólico de inicio de sesión de confianza temporal y un identificador de la página de servicio a ser accedida cumplen una primera relación de correspondencia; y

determinar si el simbólico de inicio de sesión de confianza temporal y un identificador de inicio de sesión de confianza actual emitido por el primer servidor cumplen una segunda relación de correspondencia; y

en respuesta a determinar que el simbólico de inicio de sesión de confianza temporal y el identificador de la página de servicio a ser accedida cumplen la primera relación de correspondencia y que el simbólico de inicio de sesión de confianza temporal y el identificador de inicio de sesión de confianza actual cumplen la segunda relación de correspondencia, determinar que el simbólico de inicio de sesión de confianza temporal tiene el permiso de servicio para acceder a la página de servicio.

3. El método implementado por computadora de la reivindicación 1, en donde el simbólico de inicio de sesión de confianza temporal se genera de acuerdo con una regla de generación específica para representar válido el simbólico.

4. El método implementado por computadora de la reivindicación 1, en donde el simbólico de inicio de sesión de confianza temporal expira después de un período de validez.

5. El método de la reivindicación 1, en donde el paso de determinar si el simbólico de inicio de sesión de confianza temporal tiene permiso de servicio para acceder a la página de servicio comprende:

determinar si el simbólico de inicio de sesión de confianza temporal y una identificación de servicio de la página de servicio cumplen una primera relación de correspondencia; y

si el simbólico de inicio de sesión de confianza temporal y la identificación de servicio cumplen la primera relación de correspondencia, determinar que el simbólico de inicio de sesión de confianza temporal tiene el permiso de servicio para acceder a la página de servicio.

6. El método de la reivindicación 1, en donde el paso de determinar si el simbólico de inicio de sesión de confianza temporal tiene permiso de servicio para acceder a la página de servicio comprende:

determinar si el simbólico de inicio de sesión de confianza temporal y una identificación de servicio de la página de servicio cumplen una primera relación de correspondencia, y determinar si el simbólico de inicio de sesión de confianza temporal y un identificador de inicio de sesión de confianza actual emitido por el primer servidor al segundo servidor cumplen una segunda relación de correspondencia; y

si el simbólico de inicio de sesión de confianza temporal y la identificación de servicio cumplen la primera relación de correspondencia y el simbólico de inicio de sesión de confianza temporal y el identificador de inicio de sesión de confianza actual cumplen la segunda relación de correspondencia, determinar que el simbólico de inicio de sesión de confianza temporal tiene el privilegio de servicio para acceder a la página de servicio.

7. El método de la reivindicación 1, en donde antes del paso de determinar si el simbólico de inicio de sesión de confianza temporal tiene permiso de servicio para acceder a la página de servicio, el método comprende, además:

determinar si el simbólico de inicio de sesión de confianza temporal es válido y determinar si el simbólico de inicio de sesión de confianza temporal expira; y

si el simbólico de inicio de sesión de confianza temporal es válido y no expira, realizar una operación para determinar si el simbólico de inicio de sesión de confianza temporal en base a la solicitud de acceso a la página tiene un privilegio de servicio para acceder a la página de servicio.

8. El método de la reivindicación 1, en donde la página de servicio es una página que se puede cargar en el terminal cliente de destino de forma integrada.

9. El método de cualquiera de las reivindicaciones 1, 5 a 8, que comprende, además:

recibir una solicitud de adquisición de simbólico enviada por el segundo servidor;

determinar, en base a la solicitud de adquisición de simbólico, si el terminal cliente de destino es un terminal cliente de confianza;

generar el simbólico de inicio de sesión de confianza temporal si el terminal cliente de destino es un terminal cliente de confianza, y establecer un permiso de servicio de acceso a la página para el simbólico de inicio de sesión de confianza temporal; y

enviar el simbólico de inicio de sesión de confianza temporal al terminal cliente de destino utilizando el segundo servidor.

10. El método de la reivindicación 9, en donde el paso de determinar, en base a la solicitud de adquisición de simbólico, si el terminal cliente de destino es un terminal cliente de confianza comprende:

determinar si la solicitud de adquisición de simbólico comprende el identificador de inicio de sesión de confianza actual emitido por el primer servidor al segundo servidor; y

determinar que el terminal cliente de destino es el terminal cliente de confianza si la solicitud de adquisición de simbólico comprende el identificador de inicio de sesión de confianza actual.

11. El método de la reivindicación 9, en donde el paso de determinar, en base a la solicitud de adquisición de simbólico, si el terminal cliente de destino es un terminal cliente de confianza comprende:

determinar si existe un primer terminal cliente correspondiente al terminal cliente de destino en el primer servidor; y

determinar que el terminal cliente de destino es el terminal cliente de confianza si el primer terminal cliente existe.

12. El método de la reivindicación 1, que comprende, además:

recibir, en el segundo servidor, la solicitud de inicio de sesión de confianza enviada por el terminal cliente de destino (S2.1), utilizándose la solicitud de inicio de sesión de confianza para solicitar iniciar sesión en el primer servidor y acceder a la página de servicio proporcionada por el primer servidor;

generar, mediante el segundo servidor, la solicitud de adquisición de simbólico de inicio de sesión de confianza en base a la solicitud de inicio de sesión de confianza, y enviar, desde el segundo servidor, la solicitud de adquisición de simbólico al primer servidor (S2.2), que comprende:

obtener un identificador de inicio de sesión de confianza actual emitido por el primer servidor al segundo servidor, siendo el identificador de inicio de sesión de confianza actual un certificado para obtener el simbólico de inicio de sesión de confianza temporal; y

escribir el identificador de inicio de sesión de confianza actual en la solicitud de acceso para generar la solicitud de adquisición de simbólico;

recibir, en el segundo servidor, el simbólico de inicio de sesión de confianza temporal desde el primer servidor, el simbólico de inicio de sesión de confianza temporal que tiene permiso de servicio para iniciar sesión en el primer servidor y acceder a la página de servicio, y enviar el simbólico de inicio de sesión de confianza temporal al terminal cliente de destino, de modo que el terminal cliente de destino inicie sesión en el primer servidor y acceda a la página de servicio utilizando el simbólico de inicio de sesión de confianza temporal (S2.3).

13. El método de la reivindicación 1, que comprende, además, si se determina que el simbólico de inicio de sesión de confianza temporal no tiene permiso de servicio para acceder a la correspondiente página de servicio, prohibir al terminal cliente de destino acceder a la correspondiente página de servicio.

14. Un sistema de inicio de sesión de confianza, que comprende:

un primer sistema de aplicación que incluye un primer servidor y un primer terminal cliente; y

un segundo sistema de aplicación que incluye un segundo servidor y un terminal cliente de destino;

en donde el primer servidor y el segundo servidor comprenden múltiples unidades configuradas para realizar el método de una cualquiera de las reivindicaciones 1 a 13.

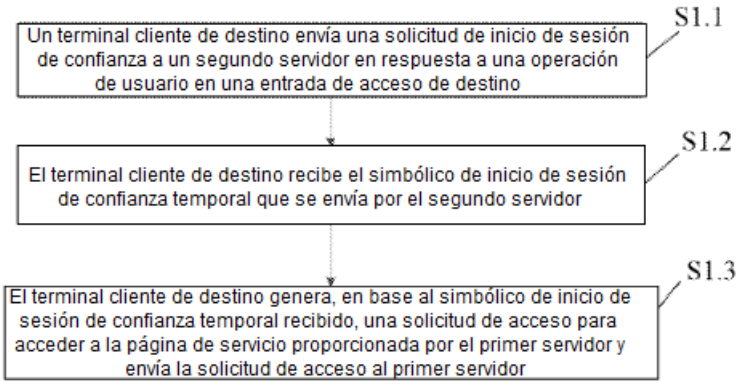

FIG. 1a

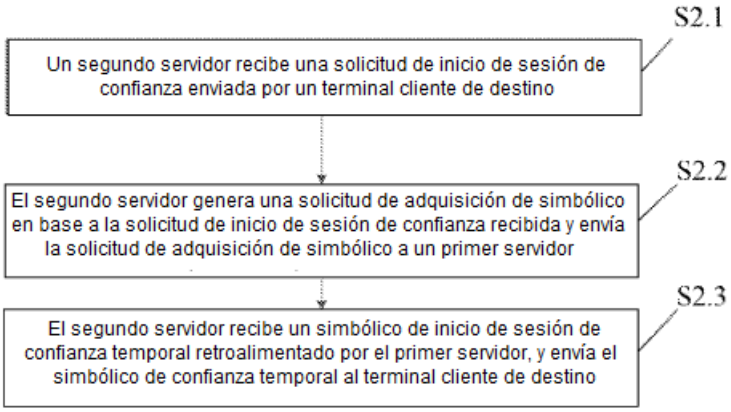

FIG. 1b

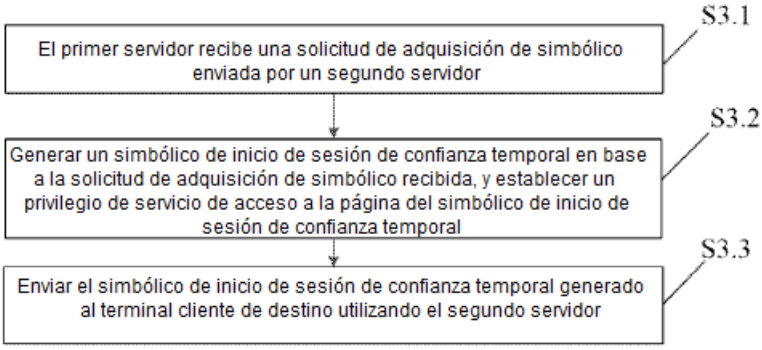

FIG. 1c

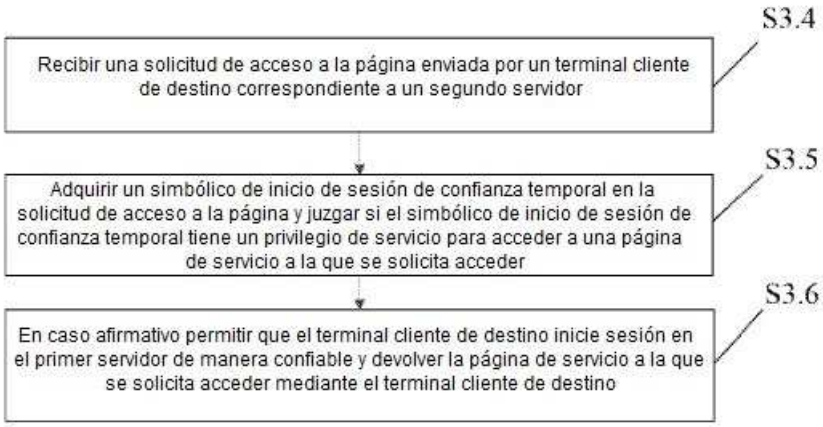
S3.4
Recibir una solicitud de acceso a la página enviada por un terminal cliente de destino correspondiente a un segundo servidor
S3.5
Adquirir un simbólico de inicio de sesión de confianza temporal en la solicitud de acceso a la página y juzgar si el simbólico de inicio de sesión de confianza temporal tiene un privilegio de servicio para acceder a una página de servicio a la que se solicita acceder
S3.6
En caso afirmativo permitir que el terminal cliente de destino inicie sesión en el primer servidor de manera confiable y devolver la página de servicio a la que se solicita acceder mediante el terminal cliente de destino

FIG. 1d

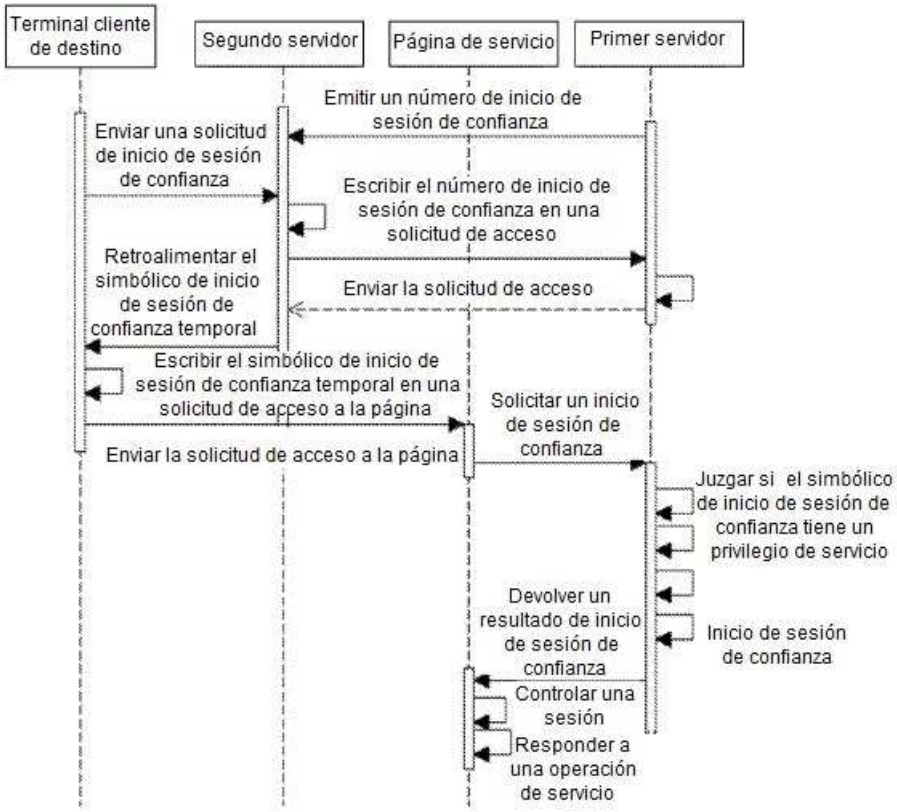
Terminal cliente de destino
Segundo servidor
Página de servicio
Primer servidor
Emitir un número de inicio de sesión de confianza
Enviar una solicitud de inicio de sesión de confianza
Escribir el número de inicio de sesión de confianza en una solicitud de acceso
Retroalimentar el simbólico de inicio de sesión de confianza temporal
Enviar la solicitud de acceso
Escribir el simbólico de inicio de sesión de confianza temporal en una solicitud de acceso a la página
Solicitar un inicio de sesión de confianza
Enviar la solicitud de acceso a la página
Juzgar si el simbólico de inicio de sesión de confianza tiene un privilegio de servicio
Devolver un resultado de inicio de sesión de confianza
Inicio de sesión de confianza
Controlar una sesión
Responder a una operación de servicio

FIG. 1e

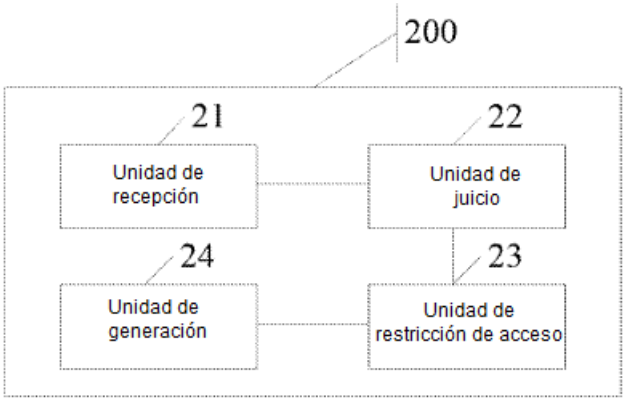

FIG. 2

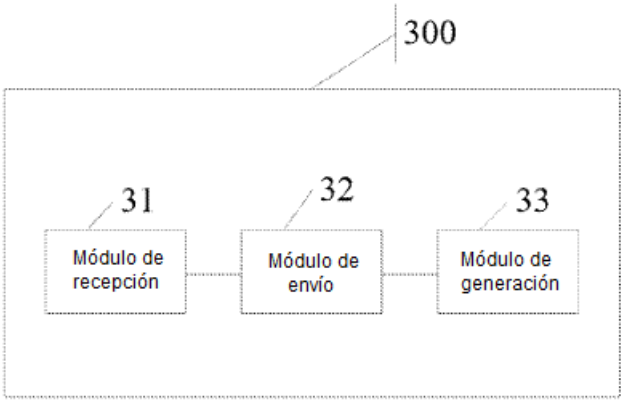

FIG. 3

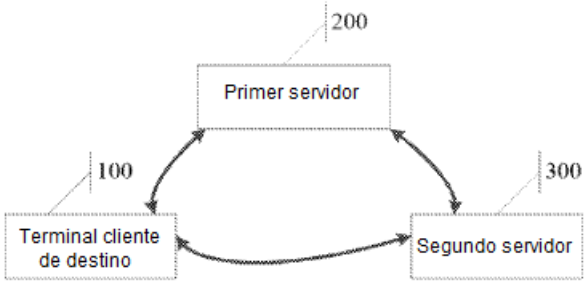

FIG. 4