(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 774 056**

(51) Int. CI.:

G06F 21/60 (2013.01)
G06F 21/33 (2013.01)
G06F 21/41 (2013.01)
G06F 21/44 (2013.01)
H04L 9/32 (2006.01)
H04W 12/06 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.05.2016 PCT/JP2016/065917**

(87) Fecha y número de publicación internacional: **07.12.2017 WO17208305**

(96) Fecha de presentación y número de la solicitud europea: **30.05.2016 E 16903933 (6)**

(97) Fecha y número de publicación de la concesión europea: **29.01.2020 EP 3346405**

(54) Título: **Dispositivo servidor, método de servicio, programa y medio de registro de información legible por ordenador no transitorio**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.07.2020

(73) Titular/es:

RAKUTEN, INC. (100.0%)
1-14-1, Tamagawa, Setagaya-ku
Tokyo 158-0094, JP

(72) Inventor/es:

KAWAI KOHEI y
KURNIAWAN SONNY

(74) Agente/Representante:

FÚSTER OLAGUIBEL, Gustavo Nicolás

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Dispositivo servidor, método de servicio, programa y medio de registro de información legible por ordenador no transitorio

Campo técnico

La presente divulgación se refiere a un dispositivo servidor, a un método de servicio, a un programa y un medio de registro de información legible por ordenador no transitorio.

Técnica anterior

Recientemente, el uso generalizado de los denominados teléfonos inteligentes ha conducido al aumento en el uso de servicios con dispositivos terminales operados por el usuario que acceden a dispositivos servidor configurados por proveedores de servicios. Cuando los servicios se proporcionan de ese modo, se requiere autenticación en algunos casos para que el dispositivo servidor identifique al usuario.

En general, para la autenticación, se usa un modo en el que un dispositivo terminal transmite a un dispositivo servidor una petición de inicio de sesión que especifica un nombre de usuario y una contraseña (inicio de sesión). En otro modo, se usa un testigo de acceso para eliminar la tarea de introducir un nombre de usuario y una contraseña cuando se proporciona de nuevo un servicio a un dispositivo terminal una vez autenticado con la petición de inicio de sesión. El testigo de acceso se registra en el dispositivo terminal y el dispositivo terminal lo transmite al dispositivo servidor para la autenticación cuando el usuario pide un servicio.

Por ejemplo, el documento de patente 1 divulga una técnica con respecto a un método de autenticación que usa testigos de acceso. Según la técnica del documento de patente 1, el servidor de autorización emite un testigo de acceso a un cesionario del derecho de acceso en respuesta a una petición de un cedente del derecho de acceso. El cesionario del derecho de acceso puede autenticarse usando el testigo de acceso emitido. La técnica del documento de patente 1 pretende permitir el acceso a la información permitida por el cedente sin hacer referencia a la información crediticia del cedente (su propio nombre de usuario y contraseña).

Lista de referencias

Bibliografía de patentes

Documento de patente 1: Publicación denominada Kokai de solicitud de patente japonesa no examinada n.º 2015-201098.

El documento US 2007/0044146 A1 da a conocer un sistema en el que se realiza el procesamiento de autenticación de usuario y se devuelve una ID de sesión de autenticación a un terminal. Un servidor de autenticación emite y almacena un vale de autenticación. El vale de autenticación y la sesión de autenticación se devuelven al terminal. Un usuario transmite una petición de prestación de servicios y el vale de autenticación al servidor de un proveedor de servicios, y el servidor del proveedor de servicios transmite el vale de autenticación al servidor de autenticación. El servidor de autenticación realiza un procesamiento de autenticación del vale de autenticación y se notifica el resultado de la autenticación. En el caso de la aprobación de autenticación, se emite una ID de sesión de servicio junto con la notificación de autorización. Cuando se recibe la notificación de la aprobación de autenticación, el terminal realiza un procesamiento de establecimiento de la sesión usando la ID de sesión de servicio recibida y almacena la ID de sesión de servicio.

Problema técnico

Sin embargo, la técnica descrita anteriormente no puede reducir la carga de trabajo del usuario requerida para la autenticación en un entorno donde se ejecutan múltiples aplicaciones en el mismo dispositivo terminal.

En un entorno en el que se ejecutan múltiples aplicaciones en el mismo dispositivo terminal, a menudo se restringe la compartición de memoria entre aplicaciones. En particular, desde el punto de vista de la seguridad, en la mayoría de los casos no se permite compartir información importante, tal como la usada en la autenticación, con otras aplicaciones. En tal caso, para usar múltiples aplicaciones con la misma información de cuenta en el mismo dispositivo terminal, el usuario debe introducir información de autenticación para cada aplicación. Por tanto, aumenta la carga de trabajo del usuario para la autenticación.

La presente divulgación se realiza en vista del problema anterior. En otras palabras, un objetivo de la divulgación es reducir la carga de trabajo del usuario requerida para la autenticación cuando un dispositivo servidor proporciona servicios al mismo dispositivo terminal en el que se ejecutan múltiples aplicaciones.

Sumario

La presente invención proporciona un dispositivo servidor según la reivindicación 1.

La presente invención también proporciona un método de servicio según la reivindicación 8.

La presente invención también proporciona un programa según la reivindicación 9.

Efectos ventajosos de la invención

La presente divulgación puede reducir la carga de trabajo del usuario requerida para la autenticación cuando un dispositivo servidor proporciona servicios al mismo dispositivo terminal en el que se ejecutan múltiples aplicaciones.

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques que muestra la configuración funcional del dispositivo servidor según una realización;

la figura 2 es un diagrama de bloques que muestra las configuraciones de hardware del dispositivo servidor y el dispositivo terminal;

la figura 3 es un diagrama de bloques que muestra la configuración funcional de una aplicación ejecutada por el dispositivo terminal;

la figura 4 es una tabla que muestra el contenido de los datos registrados en la BD de correspondencias de usuario/contraseña;

la figura 5 es una tabla que muestra el contenido de los datos registrados en la BD de testigos de acceso;

la figura 6 es un diagrama de flujo que muestra el procedimiento de petición de autenticación por el dispositivo terminal;

la figura 7 es un diagrama de flujo que muestra el procedimiento de autenticación de petición de inicio de sesión; y

la figura 8 es un diagrama de flujo que muestra el procedimiento de autenticación de petición de acceso.

Descripción de realizaciones

A continuación se describirá una realización de la presente divulgación con referencia a los dibujos.

<Realización>

Un dispositivo 100 servidor según una realización de la presente divulgación es un dispositivo servidor que proporciona servicios a un usuario a través de aplicaciones que se ejecutan en un dispositivo terminal operado por el usuario. El dispositivo 100 servidor determina si una aplicación que se ejecuta en el dispositivo terminal puede dotarse de un servicio (autenticación) y proporciona el servicio sólo cuando la aplicación se autentica como un servicio que puede proporcionarse.

El dispositivo 100 servidor comprende, tal como se muestra en la figura 1, un autenticador 10 y un proveedor 13 de servicios. El autenticador 10 es una herramienta de función que recibe una petición de autenticación desde una aplicación que se ejecuta en un dispositivo 200 terminal operado por un usuario U y que realiza autenticación para determinar si puede proporcionarse un servicio. Además, el proveedor 13 de servicios es una herramienta de función que proporciona un servicio al usuario U a través de una aplicación 31 autenticada por el autenticador 10.

El autenticador 10 comprende un autenticador 11 de inicio de sesión y un autenticador 12 de testigo de acceso como herramienta de función para autenticar la aplicación 31.

El autenticador 11 de inicio de sesión recibe desde la aplicación 31 una petición de inicio de sesión que especifica un nombre de usuario y una contraseña. El autenticador 11 de inicio de sesión autentica la aplicación 31 cuando la combinación del nombre de usuario y la contraseña incluida en la petición de inicio de sesión recibida se registra en una BD 21 de correspondencias de usuario/contraseña.

Después de autenticar la aplicación de fuente de transmisión que ha transmitido la petición de inicio de sesión (la aplicación 31), el autenticador 11 de inicio de sesión emite un testigo de acceso a la aplicación y registra el testigo de acceso en una BD 22 de testigos de acceso. El autenticador 11 de inicio de sesión transmite el testigo de acceso emitido a la aplicación de fuente de transmisión (la aplicación 31). La aplicación 31 registra el testigo de acceso

transmitido.

Para usar un servicio proporcionado por el dispositivo 100 servidor, si un testigo de acceso está almacenado en una región de almacenamiento no volátil para la aplicación 31 en el dispositivo 200 terminal, la aplicación 31 transmite una petición de acceso que especifica el testigo de acceso almacenado. Por otro lado, si no está almacenado ningún testigo de acceso en la región de almacenamiento no volátil, la aplicación 31 le pide al usuario U que introduzca un nombre de usuario y una contraseña. Cuando el usuario U introduce un nombre de usuario y una contraseña en respuesta a la petición, la aplicación 31 transmite una petición de inicio de sesión que especifica el nombre de usuario y la contraseña introducidos en el dispositivo 100 servidor.

El autenticador 12 de testigo de acceso recibe una petición de acceso que especifica un testigo de acceso desde la aplicación 31. Si el testigo de acceso incluido en la petición de acceso recibida está registrado en la BD 22 de testigos de acceso en asociación con un código de identificación de terminal que presenta el dispositivo terminal de fuente de transmisión (el dispositivo 200 terminal), el autenticador 12 de testigo de acceso autentica la aplicación 31.

Tal como se describió anteriormente, el dispositivo 100 servidor autentica la aplicación 31 mediante la combinación del autenticador 11 de inicio de sesión y el autenticador 12 de testigo de acceso. La aplicación 31 que se ejecuta en el dispositivo 200 terminal solicita al dispositivo 100 servidor la autenticación con un testigo de acceso cuando está registrado un testigo de acceso, y solicita al dispositivo 100 servidor la autenticación con un nombre de usuario y una contraseña introducidos por el usuario U cuando no está registrado ningún testigo de acceso. Por tanto, se solicita al usuario U que escriba cuando no está registrado ningún testigo de acceso (dicho de otro modo, no hay ningún registro de autenticación). Por otro lado, se usa el testigo de acceso registrado para la autenticación y se omite que el usuario U tenga que escribir cuando está registrado un testigo de acceso (dicho de otro modo, hay un registro de autenticación). Por tanto, puede reducirse la carga de trabajo del usuario U requerida para la autenticación.

El testigo de acceso son datos que comprenden una clave y una cadena de caracteres de autenticación tal como se describe más adelante. La clave es un número de identificación dado en exclusiva por el dispositivo 100 servidor como información que presenta un testigo de acceso. La cadena de caracteres de autenticación es una cadena de caracteres dada por el dispositivo 100 servidor para indicar que el testigo de acceso es legítimo. En general, el dispositivo 100 servidor facilita una cadena de caracteres aleatoria generada en condiciones específicas como cadena de caracteres de autenticación de testigo de acceso.

El dispositivo 100 servidor gestiona los testigos de acceso registrados en la BD 22 de testigos de acceso con la adición de fechas de expiración. Dicho de otro modo, incluso con una aplicación (o un dispositivo terminal) una vez autenticada y que tiene un testigo de acceso emitido, el testigo de acceso expira a menos que la aplicación (el dispositivo terminal) se autentique para una fecha de expiración dada. Cuando el testigo de acceso expira, el usuario tiene que introducir un nombre de usuario y una contraseña para la autenticación mediante un inicio de sesión con el fin de recibir el servicio desde el dispositivo 100 servidor con la aplicación o el dispositivo terminal asociado con el testigo de acceso.

Además, cuando el dispositivo 100 servidor autentica una aplicación (y un dispositivo terminal) con una petición de acceso que incluye un testigo de acceso, el dispositivo 100 servidor pospone la fecha de expiración del testigo de acceso. Por tanto, cuando el usuario recibe repetidamente un servicio desde el dispositivo 100 servidor a través de la aplicación antes de la fecha de expiración (dicho de otro modo, se autentica con un testigo de acceso), el usuario puede recibir continuamente el servicio desde el dispositivo 100 servidor sin introducir un nombre de usuario y una contraseña.

El dispositivo 200 terminal puede ejecutar aplicaciones distintas de la aplicación 31. Cuando el dispositivo 200 terminal ejecuta aplicaciones 32 y 33 usando el mismo dispositivo 100 servidor, el dispositivo 100 servidor puede autenticar las aplicaciones 31, 32 y 33 con la misma cuenta de usuario (autenticación con la combinación del mismo nombre de usuario y contraseña). Dicho de otro modo, si el dispositivo 100 servidor ha autenticado una petición de inicio de sesión transmitida por la aplicación 31 y luego la aplicación 32 transmite una petición de inicio de sesión que especifica el mismo conjunto de un nombre de usuario y una contraseña que el nombre de usuario y la contraseña especificados en esa petición de inicio de sesión, el dispositivo 100 servidor autentica la aplicación 32.

Al autenticar una aplicación, el autenticador 11 de inicio de sesión emite un testigo de acceso. El autenticador 11 de inicio de sesión registra el testigo de acceso emitido en la BD 22 de testigos de acceso y transmite el testigo de acceso emitido a la aplicación autenticada. El testigo de acceso transmitido se registra en una región de almacenamiento no volátil reservada para la aplicación por el dispositivo 200 terminal para cada aplicación autenticada. Dicho de otro modo, aunque se autentiquen múltiples aplicaciones con la misma cuenta de usuario (las aplicaciones 31, 32 y 33), el dispositivo 100 servidor emite testigos de acceso a las aplicaciones de manera individual. Las aplicaciones 31, 32 y 33 registran cada una su testigo de acceso emitido.

El dispositivo 200 terminal no permite compartir información sobre autenticación (un nombre de usuario, una contraseña, un testigo de acceso) entre aplicaciones que van a ejecutarse. Esto se debe a que la información sobre la autenticación es información muy importante en lo que se refiere a la seguridad y se pretende reducir el riesgo de

una filtración de información tan importante. Por tanto, la aplicación 31 no puede autenticarse con referencia al testigo de acceso registrado en la aplicación 32.

Por otro lado, el dispositivo 100 servidor usa datos comunes (la BD 21 de correspondencias de usuario/contraseña y la BD 22 de testigos de acceso) para autenticar múltiples aplicaciones. Por tanto, cuando la aplicación 31 que se ejecuta en el dispositivo 200 terminal accede al dispositivo 100 servidor, el dispositivo 100 servidor puede acceder a información sobre los testigos de acceso de aplicaciones que se ejecutan en el mismo dispositivo 200 terminal (las aplicaciones 32 y 33).

Específicamente, cuando el dispositivo 100 servidor autentica una petición de inicio de sesión desde la aplicación 31 a través del autenticador 11 de inicio de sesión, el dispositivo 100 servidor registra un testigo de acceso en la BD 22 de testigos de acceso en asociación con un código de identificación de terminal que presenta el dispositivo terminal en el que se ejecuta la aplicación 31 (el dispositivo 200 terminal) y con la adición de una fecha de expiración. Dicho de otro modo, el testigo de acceso se registra en la BD 22 de testigos de acceso junto con la información que presenta el dispositivo 200 terminal.

Cuando el dispositivo 100 servidor autentica una petición de inicio de sesión desde la aplicación 31, el dispositivo 100 servidor extrae un testigo de acceso emitido a una aplicación que se ejecuta en el dispositivo 200 terminal que es el mismo dispositivo terminal que la aplicación 31 y registrado en la BD 22 de testigos de acceso, y pospone la fecha de expiración del testigo de acceso extraído. Específicamente, el dispositivo 100 servidor identifica los testigos de acceso transmitidos a las aplicaciones 32 y 33 desde la BD 22 de testigos de acceso y actualiza las fechas de expiración adjuntas a fechas/momentos posteriores.

Además, cuando el dispositivo 100 servidor autentica una petición de acceso desde la aplicación 31, el dispositivo 100 servidor extrae un testigo de acceso emitido a una aplicación que se ejecuta en el dispositivo 200 terminal y registrado en la BD 22 de testigos de acceso, y pospone la fecha de expiración del testigo de acceso extraído. Específicamente, el dispositivo 100 servidor identifica los testigos de acceso transmitidos a las aplicaciones 31, 32 y 33 desde la BD 22 de testigos de acceso y actualiza las fechas de expiración adjuntas a fechas/momentos posteriores.

Al comprender la configuración descrita anteriormente, el dispositivo 100 servidor autentica aplicaciones que se ejecutan en el dispositivo 200 terminal (las aplicaciones 31, 32 y 33) y proporciona servicios a las aplicaciones autenticadas. Aunque no haya petición de autenticación (una petición de inicio de sesión o una petición de acceso) desde la aplicación 31 durante mucho tiempo, siempre que se realiza una petición de autenticación por la aplicación 32 que se ejecuta en el dispositivo 200 terminal que es el mismo dispositivo terminal antes de la fecha de expiración del testigo de acceso, se pospone la fecha de expiración del testigo de acceso emitido a la aplicación 31. Por tanto, es posible reducir la carga de trabajo del usuario requerida para la autenticación cuando un dispositivo servidor proporciona servicios al mismo dispositivo terminal en el que se ejecutan múltiples aplicaciones.

El dispositivo 100 servidor según esta realización comprende como hardware, tal como se muestra en la figura 2, un controlador 110, un dispositivo 120 de registro, un dispositivo 130 de operación, una pantalla 140 y una interfaz 150 de red. Estos están conectados entre sí mediante un bus 190 interno.

El controlador 110 comprende una unidad 111 central de procesamiento (CPU), una memoria 112 de solo lectura (ROM), una memoria 113 de acceso aleatorio (RAM), y similares. Cuando la CPU del controlador 110 ejecuta programas registrados en la ROM o la RAM, el controlador 110 controla todo el funcionamiento del dispositivo 100 servidor. El controlador 110 lee datos tales como programas del dispositivo 120 de registro según sea necesario y guarda datos en el dispositivo 120 de registro.

El dispositivo 120 de registro comprende un dispositivo de registro tal como una unidad de disco duro y una memoria flash, y almacena datos necesarios para que funcione el dispositivo 100 servidor.

El dispositivo 130 de operación comprende un teclado, un ratón, y similares, y recibe operaciones de entrada del usuario U y transmite las operaciones de entrada al controlador 110.

La pantalla 140 comprende una pantalla de cristal líquido o un monitor de tubo de rayos catódicos, y presenta visualmente información necesaria para el usuario del dispositivo 100 servidor.

La interfaz 150 de red conecta el dispositivo 100 servidor a una red. Cuando el dispositivo 100 servidor transmite información a otros dispositivos o recibe información desde otros dispositivos a través de una red, la interfaz 150 de red transmite la información recibida desde el controlador 110 a través del bus 190 interno descrito más adelante a otros dispositivos a través de una red, y transmite la información recibida desde otros dispositivos a través de una red al controlador 110 a través del bus 190 interno. Por ejemplo, el dispositivo 100 servidor transmite/recibe datos a/desde el dispositivo 200 terminal operado por el usuario U a través de la interfaz 150 de red. El usuario U se autentica y recibe servicios a través del dispositivo 200 terminal conectado al dispositivo 100 servidor a través de una red.

El dispositivo 200 terminal al que el dispositivo 100 servidor proporciona servicios comprende como hardware, tal como se muestra en la figura 2, un controlador 210, un dispositivo 220 de registro, un panel 230 táctil y una interfaz 250 de red. Estos están conectados entre sí mediante un bus 290 interno.

El controlador 210 comprende una CPU 211, una ROM 212, una RAM 213, y similares. Cuando la CPU del controlador 210 ejecuta programas registrados en la ROM o la RAM, el controlador 210 controla todo el funcionamiento del dispositivo 200 terminal.

El dispositivo 220 de registro comprende un dispositivo de registro tal como una unidad de disco duro y una memoria flash, y almacena datos necesarios para que funcione el dispositivo 200 terminal.

El panel 230 táctil es un dispositivo electrónico en el que se combinan una pantalla que puede presentar visualmente información y un dispositivo de detección de posición que detecta un punto tocado. El panel 230 táctil recibe operaciones de entrada por parte del usuario U por medio del dispositivo de detección de posición y transmite las operaciones de entrada al controlador 210. Además, el panel 230 táctil presenta visualmente información necesaria para el usuario U por medio de la pantalla.

La interfaz 250 de red conecta el dispositivo 200 terminal a una red. En particular, el dispositivo 200 terminal transmite/recibe datos a/desde el dispositivo 100 servidor a través de la interfaz 250 de red.

La aplicación 31 ejecutada por el dispositivo 200 terminal comprende los componentes mostrados en la figura 3. Dicho de otro modo, la aplicación 31 comprende, como herramientas de función, un receptor 31a de servicio que recibe un servicio desde el proveedor 13 de servicios del dispositivo 100 servidor y un autenticador 31b que se somete a autenticación por el dispositivo 100 servidor. Además, la aplicación 31 registra un testigo 31c de acceso en una región de almacenamiento no volátil del dispositivo 200 terminal que se asigna a la aplicación 31. El testigo 31c de acceso comprende una clave 31ca y una cadena 31cb de caracteres de autenticación.

La clave 31ca es información de identificación dada en exclusiva por el dispositivo 100 servidor para identificar el testigo de acceso.

La cadena 31cb de caracteres de autenticación es una cadena de caracteres emitida por el dispositivo 100 servidor en asociación con la clave, de modo que el testigo de acceso no se use incorrectamente. En la generación de un testigo de acceso, el dispositivo 100 servidor genera una clave que sirve como información de identificación como información única y añade a la clave una cadena de caracteres aleatoria generada en condiciones específicas para generar un testigo de acceso.

El testigo de acceso se emite y se gestiona por el dispositivo 100 servidor en la base de aplicación. Cuando el autenticador 31b realiza una petición de inicio de sesión usando un nombre de usuario y una contraseña y se aprueba la petición de inicio de sesión, la aplicación 31 registra un testigo de acceso transmitido por el dispositivo 100 servidor sin ningún cambio. La aplicación 31 registra y transmite el testigo 31c de acceso pero no corrige datos.

Puesto que el dispositivo 100 servidor emite testigos de acceso en la base de aplicación, la aplicación 31 y la aplicación 32 registran cada una en exclusiva un testigo de acceso. Dicho de otro modo, el testigo de acceso registrado por la aplicación 31 y el testigo de acceso registrado por la aplicación 32 se registran independientemente y sus contenidos no son iguales.

La aplicación 31 puede no registrar datos relacionados con la autenticación aparte del testigo 31c de acceso. Si el testigo 31c de acceso no está registrado o si el testigo 31c de acceso registrado no es válido, la aplicación 31 solicita que el usuario introduzca un nombre de usuario y una contraseña y transmite el nombre de usuario y contraseña introducidos al dispositivo 100 servidor. Sin embargo, después no se hará referencia al nombre de usuario y a la contraseña transmitidos.

El dispositivo 100 servidor registra datos mostrados en la figura 4 en la BD 21 de correspondencias de usuario/contraseña. Dicho de otro modo, el dispositivo 100 servidor registra nombres de usuario y contraseñas asociados con los nombres de usuario en la BD 21 de correspondencias de usuario/contraseña.

En este caso, en la figura 4, se muestran cadenas de caracteres que presentan las contraseñas tal como son. Sin embargo, es deseable registrar en la BD 21 de correspondencias de usuario/contraseña las cadenas de caracteres que presentan las contraseñas (o información correspondiente a las mismas) en un formato que garantice la seguridad. Por ejemplo, en la BD 21 de correspondencias de usuario/contraseña pueden registrarse cadenas de caracteres generadas mediante cifrado de las cadenas de caracteres de las contraseñas introducidas por los usuarios. En tal caso, para determinar si una cadena de caracteres introducida por el usuario coincide con la contraseña establecida, el dispositivo 100 servidor decodifica una contraseña cifrada registrada en la BD 21 de correspondencias de usuario/contraseña y determina si la cadena de caracteres introducida por el usuario coincide con la contraseña establecida.

Alternativamente, los valores resumen de las contraseñas introducidas por los usuarios pueden registrarse en la BD 21 de correspondencias de usuario/contraseña. En tal caso, para registrar la información correspondiente a una cadena de caracteres que presenta una contraseña, el dispositivo 100 servidor registra en la BD 21 de correspondencias de usuario/contraseña información generada mediante el uso de una función resumen basada en la cadena de caracteres que presenta la contraseña. Para determinar si una cadena de caracteres introducida por el usuario coincide con la contraseña establecida, el dispositivo 100 servidor determina si la información generada mediante el uso de una función resumen basada en la cadena de caracteres introducida por el usuario coincide con la información registrada en la BD 21 de correspondencias de usuario/contraseña. Además, el dispositivo 100 servidor puede registrar en la BD 21 de correspondencias de usuario/contraseña información generada mediante el uso de una función resumen basada en una cadena de caracteres obtenida añadiendo una cadena de caracteres denominada sal a una cadena de caracteres establecida por el usuario como contraseña (un valor resumen) en asociación con la sal.

El dispositivo 100 servidor registra datos mostrados en la figura 5 en la BD 22 de testigos de acceso. El dispositivo 100 servidor registra en la BD 22 de testigos de acceso información tal como un testigo de acceso que incluye una clave y una cadena de caracteres de autenticación, una ID de aplicación que es un número de identificación que presenta una aplicación, un nombre de usuario, una fecha de expiración dada al testigo de acceso, y un código de identificación de terminal que presenta un dispositivo terminal.

En la figura 5, la cadena de caracteres de autenticación de un testigo de acceso es una cadena aleatoria de 12 caracteres que comprende 12 caracteres alfanuméricos. Sin embargo, esto no es restrictivo y pueden usarse cadenas de caracteres aleatorias más largas como cadena de caracteres de autenticación.

Al autenticar una aplicación mediante el inicio de sesión, el dispositivo 100 servidor emite un testigo de acceso y registra el testigo de acceso en la BD 22 de testigos de acceso. Además, al hacer esto, el dispositivo 100 servidor registra una ID de aplicación que presenta la aplicación de fuente de transmisión que ha pedido la autenticación de inicio de sesión, un nombre de usuario autenticado por el inicio de sesión, y un código de identificación de terminal del dispositivo terminal en el que se ejecuta la aplicación de fuente de transmisión en asociación con el testigo de acceso. Además, tras la autenticación, el dispositivo 100 servidor da una fecha de expiración al testigo de acceso y registra la fecha de expiración dada en la BD 22 de testigos de acceso.

El procedimiento de petición de autenticación, que es el primer procedimiento que va a ejecutarse cuando la aplicación 31 se inicia en el dispositivo 200 terminal, se describirá con referencia a la figura 6. Cuando el usuario U realiza una operación de inicio, la aplicación 31 inicia el procedimiento de petición de autenticación.

En primer lugar, la aplicación 31 determina si un testigo de acceso está registrado en la región de almacenamiento no volátil asignada a la aplicación 31 en el dispositivo 200 terminal (etapa S11).

Si en la etapa S11 se determina que no está registrado ningún testigo de acceso (etapa S11: NO), la aplicación 31 pide al usuario que introduzca un nombre de usuario y una contraseña (etapa S12). La aplicación 31 presenta visualmente una forma para introducir un nombre de usuario y una contraseña e insta al usuario para que escriba a través del panel 230 táctil del dispositivo 200 terminal.

Cuando el usuario introduce un nombre de usuario y una contraseña, la aplicación 31 transmite una petición de inicio de sesión al dispositivo 100 servidor (etapa S13). La aplicación 31 transmite al dispositivo 100 servidor una petición de inicio de sesión que especifica el nombre de usuario y la contraseña introducida por el usuario.

Entonces, la aplicación 31 determina si el dispositivo 100 servidor aprueba el acceso (etapa S14). La aplicación 31 recibe una señal transmitida por el dispositivo 100 servidor en respuesta a la petición de inicio de sesión transmitida y determina si la señal recibida indica aprobación de acceso o denegación de acceso.

Si en la etapa S14 se determina que el dispositivo 100 servidor aprueba el acceso (etapa S14: SÍ), la aplicación 31 guarda un testigo de acceso (etapa S15). Cuando el dispositivo 100 servidor aprueba el acceso en respuesta a una petición de inicio de sesión, el dispositivo 100 servidor transmite a la aplicación 31 un testigo de acceso además de la señal que indica la aprobación de acceso tal como se describió anteriormente. La aplicación 31 recibe el testigo de acceso transmitido por el dispositivo 100 servidor y registra el testigo de acceso en la región de almacenamiento no volátil.

Posteriormente, la aplicación 31 inicia el uso de un servicio por parte del usuario (etapa S16). La aplicación 31 se conecta al proveedor 13 de servicios del dispositivo 100 servidor a través del receptor 31a de servicio. A partir de entonces, mientras continúa el uso del servicio desde el dispositivo 100 servidor por parte del usuario U, la aplicación 31 finaliza el procedimiento de petición de autenticación.

Si en la etapa S14 se determina que el dispositivo 100 servidor no aprueba el acceso (etapa S14: NO), se notificará al usuario la denegación del uso del servicio (etapa S17). Cuando el dispositivo 100 servidor no aprueba el acceso

en respuesta a una petición de inicio de sesión, el dispositivo 100 servidor transmite una señal que indica la denegación de acceso a la aplicación 31. Al recibir la señal que indica la denegación de acceso desde el dispositivo 100 servidor, la aplicación 31 notifica al usuario U la denegación de prestación del servicio (autenticación no satisfactoria). Al terminar la etapa S17, la aplicación 31 finaliza el procedimiento de petición de autenticación.

Por otro lado, si en la etapa S11 se determina que un testigo de acceso está registrado (etapa S11: SÍ), la aplicación 31 transmite una petición de acceso con el testigo de acceso registrado al dispositivo 100 servidor (etapa S18). La aplicación 31 transmite al dispositivo 100 servidor el testigo de acceso registrado con la adición de un código de identificación de terminal que presenta el dispositivo 200 terminal.

Entonces, la aplicación 31 determina si el dispositivo 100 servidor aprueba el acceso (etapa S19). La aplicación 31 recibe una señal transmitida por el dispositivo 100 servidor en respuesta a la petición de acceso transmitida y determina si la señal recibida indica aprobación de acceso o denegación de acceso.

Si en la etapa S19 se determina que el dispositivo 100 servidor aprueba el acceso (etapa S19: SÍ), la aplicación 31 cambia el procesamiento a la etapa S16 descrita anteriormente e inicia el uso de un servicio por parte del usuario (etapa S16). La aplicación 31 se conecta al proveedor 13 de servicios del dispositivo 100 servidor a través del receptor 31a de servicio. A partir de entonces, mientras continúa el uso del servicio desde el dispositivo 100 servidor por parte del usuario U, la aplicación 31 finaliza el procedimiento de petición de autenticación.

Si en la etapa S19 se determina que el dispositivo 100 servidor no aprueba el acceso (etapa S19: NO), la aplicación 31 cambia el procesamiento a la etapa S17 descrita anteriormente y notifica al usuario la denegación de uso del servicio (etapa S17). Cuando el dispositivo 100 servidor no aprueba el acceso en respuesta a una petición de acceso, el dispositivo 100 servidor transmite una señal que indica la denegación de acceso a la aplicación 31. Al recibir la señal que indica la denegación de acceso desde el dispositivo 100 servidor, la aplicación 31 notifica al usuario U la denegación de prestación del servicio (autenticación no satisfactoria). Al terminar la etapa S17, la aplicación 31 finaliza el procedimiento de petición de autenticación.

Al ejecutar el procedimiento de petición de autenticación descrito anteriormente, el dispositivo 200 terminal transmite una petición de inicio de sesión o una petición de acceso al dispositivo 100 servidor e inicia el uso de un servicio sólo cuando se aprueba el acceso. A continuación en el presente documento se describirá el procedimiento de autenticación (el procedimiento de autenticación de petición de inicio de sesión y el procedimiento de autenticación de petición de acceso) ejecutado por el dispositivo 100 servidor para abordar el procedimiento de petición de autenticación del dispositivo 200 terminal.

Al recibir una petición de inicio de sesión desde la aplicación 31, el dispositivo 100 servidor inicia el procedimiento de autenticación de petición de inicio de sesión mostrado en la figura 7.

Al comienzo del procedimiento de autenticación de petición de inicio de sesión, el dispositivo 100 servidor extrae un nombre de usuario y una contraseña de la petición de inicio de sesión recibida (etapa S21). El dispositivo 100 servidor extrae un nombre de usuario y una contraseña de la petición de inicio de sesión recibida y los identifica como el nombre de usuario y la contraseña especificados por la petición de inicio de sesión.

Entonces, el dispositivo 100 servidor determina si la contraseña extraída está registrada en la BD 21 de correspondencias de usuario/contraseña en asociación con el nombre de usuario extraído (etapa S22), el dispositivo 100 servidor busca en la BD 21 de correspondencias de usuario/contraseña basándose en el nombre de usuario extraído y determina si la contraseña registrada en asociación con el nombre de usuario extraído coincide con la contraseña extraída.

Si en la etapa S22 se determina que la contraseña extraída no está registrada en asociación con el nombre de usuario extraído (etapa S22: NO), el dispositivo 100 servidor transmite la denegación de acceso a la aplicación 31 (etapa S27). Posteriormente, el dispositivo 100 servidor finaliza el procedimiento de autenticación de petición de inicio de sesión.

Por otro lado, si se determina que la contraseña extraída está registrada en asociación con el nombre de usuario extraído en la etapa S22 (etapa S22: SÍ), el dispositivo 100 servidor emite un testigo de acceso (etapa S23). El dispositivo 100 servidor genera y concatena una clave y una cadena de caracteres de autenticación de un testigo de acceso y emite el testigo de acceso.

Entonces, el dispositivo 100 servidor transmite a la aplicación 31 la aprobación de acceso y el testigo de acceso emitido (etapa S24). El dispositivo 100 servidor transmite a la aplicación 31 una señal que indica la aprobación de acceso y el testigo de acceso emitido en la etapa S23.

Entonces, el dispositivo 100 servidor registra el testigo de acceso emitido con la adición de una fecha de expiración (etapa S25). El dispositivo 100 servidor concatena y registra en la BD 22 de testigos de acceso como un único registro el testigo de acceso emitido, la información que presenta la fecha de expiración, una ID de aplicación que

presenta la aplicación 31, y un código de identificación de terminal que presenta el dispositivo terminal en el que se ejecuta la aplicación 31 (el dispositivo 200 terminal).

Entonces, el dispositivo 100 servidor pospone las fechas de expiración de otros testigos de acceso que tienen el mismo código de identificación de terminal (etapa S26). El dispositivo 100 servidor lee de la BD 22 de testigos de acceso todos los registros en los que está registrado el código de identificación de terminal del dispositivo 200 terminal. El dispositivo 100 servidor pospone las fechas de expiración registradas en los registros distingos del registro registrado en la etapa S25 entre los registros leídos. Al terminar la etapa S26, el dispositivo 100 servidor finaliza el procedimiento de autenticación de petición de inicio de sesión.

Anteriormente se ha descrito el procedimiento de autenticación cuando el dispositivo 100 servidor recibe una petición de inicio de sesión desde la aplicación 31. A continuación en el presente documento se describirá el procedimiento de autenticación cuando el dispositivo 100 servidor recibe una petición de acceso con un testigo de acceso desde la aplicación 31 con referencia a la figura 8. Al recibir una petición de acceso desde la aplicación 31, el dispositivo 100 servidor inicia el procedimiento de autenticación de petición de acceso mostrado en la figura 8.

Al comienzo del procedimiento de autenticación de petición de acceso, el dispositivo 100 servidor identifica el código de identificación de terminal del dispositivo terminal que es la fuente de transmisión de la petición de acceso recibida (etapa S31). El dispositivo 100 servidor extrae un código de identificación de terminal que presenta el dispositivo terminal de fuente de transmisión (el dispositivo 200 terminal) de la petición de acceso.

Entonces, el dispositivo 100 servidor extrae un testigo de acceso de la petición de acceso recibida (etapa S32). El dispositivo 100 servidor extrae una parte correspondiente a un testigo de acceso de la petición de acceso recibida.

Entonces, el dispositivo 100 servidor determina si el testigo de acceso extraído está registrado de manera válida en la BD 22 de testigos de acceso (etapa S33). El dispositivo 100 servidor lee de la BD 22 de testigos de acceso el testigo de acceso extraído en la etapa S32 y determina si ha pasado la fecha de expiración dada al testigo de acceso. El dispositivo 100 servidor determina que el testigo de acceso extraído no está registrado de manera válida en la BD 22 de testigos de acceso (1) cuando el testigo de acceso extraído no está registrado en la BD 22 de testigos de acceso o (2) cuando el testigo de acceso extraído está registrado en la BD 22 de testigos de acceso pero ha expirado.

Si en la etapa S33 se determina que el testigo de acceso extraído no está registrado de manera válida en la BD 22 de testigos de acceso (etapa S33: NO), el dispositivo 100 servidor transmite la denegación de acceso a la aplicación 31 (etapa S36). Posteriormente, el dispositivo 100 servidor finaliza el procedimiento de autenticación de petición de acceso.

Por otro lado, si en la etapa S33 se determina que el testigo de acceso extraído está registrado de manera válida en la BD 22 de testigos de acceso (etapa S33: SÍ), el dispositivo 100 servidor transmite la aprobación de acceso a la aplicación 31 (etapa S34). El dispositivo 100 servidor transmite una señal que indica la aprobación de acceso a la aplicación 31.

Entonces, el dispositivo 100 servidor pospone las fechas de expiración de todos los testigos de acceso que tienen el código de identificación de terminal identificado en la etapa S31 (etapa S35). En la etapa S31, el dispositivo 100 servidor lee de la BD 22 de testigos de acceso todos los registros en los que está registrado el código de identificación de terminal identificado. El dispositivo 100 servidor pospone las fechas de expiración registradas en todos los registros leídos. Al terminar la etapa S35, el dispositivo 100 servidor finaliza el procedimiento de autenticación de petición de acceso.

Cuando el dispositivo 100 servidor autentica la aplicación 31 mediante los dos procedimientos de autenticación descritos anteriormente (el procedimiento de autenticación de petición de inicio de sesión y el procedimiento de autenticación de petición de acceso), el dispositivo 100 servidor pospone las fechas de expiración de los testigos de acceso de las aplicaciones 32 y 33 que se ejecutan en el mismo dispositivo terminal que la aplicación 31 (el dispositivo 200 terminal). Como resultado, puede eliminarse la entrada de un nombre de usuario y una contraseña cuando el usuario U recibe un servicio con la aplicación 32 ó 33.

En esta realización, el dispositivo 100 servidor gestiona las fechas de expiración de los testigos de acceso y por tanto, no es necesario que las aplicaciones que se ejecutan en el dispositivo 200 terminal compartan información. Por tanto, incluso en un entorno donde se restringe la compartición de memoria entre aplicaciones en el dispositivo 200 terminal y la aplicación 31 y la aplicación 32 no pueden acceder a los mismos datos, el dispositivo 100 servidor puede posponer la fecha de expiración del testigo de acceso emitido a la aplicación 32 junto con la autenticación de la aplicación 31.

Anteriormente se ha descrito una realización de la presente divulgación. La presente divulgación no se restringe al contenido descrito anteriormente. Por ejemplo, pueden realizarse las siguientes modificaciones.

En el procedimiento de autenticación de petición de acceso mostrado en la figura 8, si en la etapa S33 se determina que el testigo de acceso no está registrado de manera válida en la BD 22 de testigos de acceso, el dispositivo 100 servidor transmite la denegación de acceso a la aplicación 31 (etapa S36) y finaliza el procedimiento. Sin embargo, el dispositivo 100 servidor no solo puede denegar simplemente el acceso, sino también ordenar a la aplicación 31 de fuente de transmisión que transmita una petición de inicio de sesión.

La aplicación 31 no maneja información con respecto a la fecha de expiración de un testigo de acceso registrado y por tanto retiene el testigo de acceso tal como está después de que el testigo de acceso ha expirado. Entonces, cuando la aplicación 31 transmite un testigo de acceso expirado al dispositivo 100 servidor, el dispositivo 100 servidor ordena a la aplicación 31 que transmita una petición de inicio de sesión, notificando de ese modo la aplicación 31 que el testigo de acceso retenido ya no es válido. La aplicación 31 elimina el testigo de acceso registrado, solicita al usuario que introduzca un nombre de usuario y una contraseña, y transmite al dispositivo 100 servidor una petición de inicio de sesión que especifica el nombre de usuario y la contraseña introducidos. Autenticada con la petición de inicio de sesión, la aplicación 31 puede recibir un testigo de acceso válido desde el dispositivo 100 servidor.

Además, al dar una orden para transmitir una petición de inicio de sesión, el dispositivo 100 servidor puede extraer un nombre de usuario del registro que presenta el testigo de acceso en la BD 22 de testigos de acceso (cuando el testigo de acceso está registrado como expirado), y transmitir el nombre de usuario extraído a la aplicación 31. Presentando el nombre de usuario recibido al solicitar al usuario que introduzca un nombre de usuario y una contraseña, el dispositivo 200 terminal puede sugerir al usuario con qué nombre de usuario debe iniciar sesión el usuario.

Cuando se autentica una petición de acceso (o una petición de inicio de sesión) desde la aplicación 31, el dispositivo 100 servidor según esta realización pospone la fecha de expiración de un testigo de acceso emitido a otra aplicación (la aplicación 32) que se ejecuta en el mismo dispositivo terminal (el dispositivo 200 terminal). Con respecto a esto, la fecha de expiración puede posponerse en cualquier modo.

Por ejemplo, se supone que el dispositivo 100 servidor autentica una petición de acceso desde la aplicación 31 y pospone la fecha de expiración dada al testigo de acceso emitido a la aplicación 31 en un primer periodo, y como resultado la fecha de expiración dada a la aplicación 31 se establece en una primera fecha de expiración. Además, se supone que el plazo de validez restante del testigo de acceso emitido a la aplicación 31 antes de la ampliación es un segundo periodo. Entonces, el dispositivo 100 servidor puede posponer la fecha de expiración del testigo de acceso emitido a la aplicación 32 mediante los métodos siguientes:

(1) establecer la fecha de expiración para la misma fecha/momento que la nueva fecha de expiración del testigo de acceso emitido a la aplicación 31 (la primera fecha de expiración);

(2) posponer la fecha de expiración en un periodo correspondiente al periodo en que se pospone el testigo de acceso emitido a la aplicación 31 (el primer periodo); o

(3) siempre que el dispositivo 100 servidor amplíe el plazo de validez dado al testigo de acceso emitido a la aplicación 31 en un primer factor de multiplicación (el primer factor de multiplicación = (el primer periodo + el segundo periodo) / el segundo periodo), ampliar el plazo de modo que el plazo de validez restante se amplíe en el primer factor de multiplicación en comparación con antes de la ampliación.

Como ejemplo del método (1) anterior, se supone que el dispositivo 100 servidor da una nueva fecha de expiración 31/3/2016 al testigo de acceso emitido a la aplicación 31. En tal caso, el dispositivo 100 servidor da la misma fecha/momento (31/3/2016) al testigo de acceso emitido a la aplicación 32 como fecha de expiración.

Como ejemplo del método (2) anterior, se supone que el dispositivo 100 servidor pospone la fecha de expiración del testigo de acceso emitido a la aplicación 31 en 10 días. En tal caso, el dispositivo 100 servidor pospone la fecha de expiración del testigo de acceso emitido a la aplicación 32 en el mismo periodo (10 días).

Como ejemplo del método (3) anterior, se supone que el plazo de validez restante del testigo de acceso emitido a la aplicación 31 antes de la ampliación es de cinco días y el dispositivo 100 servidor amplía el plazo en 10 días. En tal caso, el dispositivo 100 servidor amplía el plazo de validez del testigo de acceso emitido a la aplicación 31 en un factor de multiplicación de 3 (= 15/5). Cuando el plazo de validez restante del testigo de acceso emitido a la aplicación 32 antes de la ampliación es de siete días, el dispositivo 100 servidor amplía el plazo de validez en 14 días de modo que el plazo de validez restante se amplía en un factor de multiplicación de 3 en comparación con antes de la ampliación.

El dispositivo servidor según la realización de la presente divulgación puede realizarse también por un sistema informático convencional, no por un sistema dedicado. Por ejemplo, los programas para realizar las operaciones anteriores pueden almacenarse y distribuirse en un medio de registro legible por ordenador no transitorio, tal como un disco flexible, un disco compacto de memoria de solo lectura (CD-ROM), un disco versátil digital (DVD) y un disco

magnetoóptico (MO) e instalarse en un sistema informático para configurar un sistema de análisis de programa fuente que ejecuta los procedimientos descritos anteriormente. Además, los programas pueden almacenarse en una unidad de disco o similar de un dispositivo servidor en Internet y, por ejemplo, superponerse en ondas portadoras y descargarse en un ordenador.

Además, el dispositivo servidor según la realización de la presente divulgación no se realiza necesariamente por un solo dispositivo. Múltiples ordenadores pueden hacerse cargo de algunas de las funciones descritas anteriormente y proporcionar las funciones como un solo sistema que comprende los múltiples ordenadores.

Por tanto, esta descripción detallada, no debe considerarse en sentido limitativo, y el alcance de la invención se define sólo por las reivindicaciones incluidas, junto con el ámbito total de equivalentes al que dan derecho tales reivindicaciones.

Lista de signos de referencia

10	Autenticador
11	Autenticador de inicio de sesión
12	Autenticador de testigo de acceso
13	Proveedor de servicios
21	BD de correspondencia de usuario/contraseña BD
22	BD de testigos de acceso
31	Aplicación
31a	Receptor de servicio
31b	Autenticador
31c	Testigo de acceso
32	Aplicación
33	Aplicación
100	Dispositivo servidor
110	Controlador
111	CPU
112	ROM
113	RAM
120	Dispositivo de registro
130	Dispositivo de operación
140	Pantalla
150	Interfaz de red
190	Bus interno
200	Dispositivo terminal
210	Controlador
211	CPU
212	ROM

213	RAM
220	Dispositivo de registro
230	Panel táctil
250	Interfaz de red
290	Bus interno
U	Usuario

REIVINDICACIONES

1. Dispositivo (100) servidor configurado para recibir acceso desde múltiples aplicaciones (31, 32, 33) que se ejecutan en un dispositivo (200) terminal, en el que el dispositivo servidor está configurado adicionalmente para:

recibir desde al menos una aplicación de las múltiples aplicaciones (31, 32, 33) una petición de inicio de sesión que especifica un nombre de usuario y una contraseña introducidos por un usuario (U) del dispositivo (200) terminal cuando un testigo de acceso emitido a la aplicación (31, 32, 33) no está almacenado en una región de almacenamiento no volátil reservada para la aplicación (31, 32, 33) por el dispositivo (200) terminal, y

recibir, desde al menos una aplicación de las múltiples aplicaciones (31, 32, 33), una petición de acceso que especifica un testigo de acceso emitido a la aplicación (31, 32, 33) cuando el testigo de acceso no está almacenado en la región de almacenamiento no volátil,

realizar autenticación con el nombre de usuario y la contraseña especificados en la petición de inicio de sesión cuando se recibe la petición de inicio de sesión transmitida por cualquiera de las aplicaciones (31) que se ejecutan en el dispositivo (200) terminal,

emitir el testigo de acceso asociado con el nombre de usuario especificado en la petición de inicio de sesión a una aplicación (31) de fuente de transmisión que ha transmitido la petición de inicio de sesión si la autenticación es satisfactoria, y transmitir el testigo de acceso emitido a la aplicación (31) de fuente de transmisión, y aprobar el acceso desde la aplicación (31) de fuente de transmisión;

almacenar el testigo de acceso emitido en asociación con un código de identificación de terminal que presenta el dispositivo (200) terminal en el que se ejecuta la aplicación (31) de fuente de transmisión que ha transmitido la petición de inicio de sesión y con la adición de una fecha de expiración, y posponer las fechas de expiración dadas a otros testigos de acceso almacenados en asociación con el código de identificación de terminal; y

aprobar el acceso desde una aplicación (31) de fuente de transmisión que ha transmitido la petición de acceso y posponer las fechas de expiración dadas a todos los testigos de acceso almacenados en asociación con el código de identificación de terminal del dispositivo (200) terminal en el que se ejecuta la aplicación (31) de fuente de transmisión, cuando se recibe la petición de acceso transmitida por cualquiera de las aplicaciones (31) que se ejecutan en el dispositivo (200) terminal y el testigo de acceso especificado en la petición de acceso está almacenado en asociación con el código de identificación de terminal y como no expirado.

2. Dispositivo (100) servidor según la reivindicación 1, en el que

el dispositivo (100) servidor está configurado adicionalmente para ordenar a la aplicación (31) de fuente de transmisión que transmita la petición de inicio de sesión cuando el testigo de acceso especificado en la petición de acceso recibida no está almacenado o ha pasado la fecha de expiración almacenada.

3. Dispositivo (100) servidor según la reivindicación 2, en el que

el dispositivo (100) servidor está configurado adicionalmente para:

almacenar el testigo de acceso emitido en asociación con una combinación del código de identificación de terminal y el nombre de usuario especificado en la petición de inicio de sesión y con la adición de la fecha de expiración, y

transmitir el nombre de usuario incluido en la combinación que incluye el código de identificación de terminal a la aplicación (31) de fuente de transmisión y ordenar a la aplicación (31) de fuente de transmisión que transmita la petición de inicio de sesión cuando el testigo de acceso especificado en la petición de acceso recibida está almacenado en asociación con el código de identificación de terminal del dispositivo (200) terminal en el que se ejecuta la aplicación (31) de fuente de transmisión que ha transmitido la petición de acceso y como expirado.

4. Dispositivo (100) servidor según la reivindicación 1, en el que

cuando el testigo de acceso especificado en la petición de acceso recibida está almacenado en asociación con el código de identificación de terminal del dispositivo (200) terminal en el que se ejecuta la aplicación (31) de fuente de transmisión que ha transmitido la petición de acceso y como no expirado y se pospone la fecha de expiración del testigo de acceso emitida a la aplicación (31) de fuente de transmisión hasta una

primera fecha de expiración, el dispositivo (100) servidor está configurado para posponer las fechas de expiración dadas a todos los testigos de acceso emitidos a las otras aplicaciones (32, 33) y almacenados en asociación con el código de identificación de terminal hasta la primera fecha de expiración.

5. Dispositivo (100) servidor según la reivindicación 1, en el que

cuando el testigo de acceso especificado en la petición de acceso recibida está almacenado en asociación con el código de identificación de terminal del dispositivo (200) terminal en el que se ejecuta la aplicación (31) de fuente de transmisión que ha transmitido la petición de acceso y como no expirado y se pospone la fecha de expiración del testigo de acceso emitido a la aplicación (31) de fuente de transmisión en un primer periodo, el dispositivo (100) servidor está configurado para posponer las fechas de expiración dadas a todos los testigos de acceso emitidos a las otras aplicaciones (32, 33) y almacenados en asociación con el código de identificación de terminal en el primer periodo.

6. Dispositivo (100) servidor según la reivindicación 1, en el que

cuando el testigo de acceso especificado en la petición de acceso recibida está almacenado en asociación con el código de identificación de terminal del dispositivo (200) terminal en el que se ejecuta la aplicación (31) de fuente de transmisión que ha transmitido la petición de acceso y como no expirado y se amplía un plazo de validez del testigo de acceso emitido a la aplicación (31) de fuente de transmisión de modo que un plazo de validez restante del testigo de acceso se amplía en un primer factor de multiplicación en comparación con antes de la ampliación, el dispositivo (100) servidor está configurado para ampliar los plazos de validez dados a todos los testigos de acceso emitidos a las otras aplicaciones (32, 33) y almacenados en asociación con el código de identificación de terminal de modo que los plazos de validez restantes se amplían en el primer factor de multiplicación en comparación con antes de la ampliación.

7. Sistema que comprende múltiples aplicaciones (31, 32, 33) configuradas para ejecutarse en un dispositivo (200) terminal y el dispositivo (100) servidor según la reivindicación 1, en el que:

cada una de las múltiples aplicaciones está configurada para:

solicitar a un usuario (U) que introduzca un nombre de usuario y una contraseña y que transmita una petición de inicio de sesión que especifica el nombre de usuario y la contraseña introducidos en el dispositivo (100) servidor cuando un testigo de acceso emitido a la aplicación (31, 32, 33) no está almacenado en una región de almacenamiento no volátil reservada para la aplicación (31, 32, 33) por el dispositivo (200) terminal; y

transmitir al dispositivo (100) servidor una petición de acceso que especifica un testigo de acceso emitido a la aplicación (31, 32, 33) cuando el testigo de acceso está almacenado en la región de almacenamiento no volátil.

8. Método de servicio por un dispositivo (100) servidor que recibe acceso desde múltiples aplicaciones (31, 32, 33) que se ejecutan en un dispositivo (200) terminal, comprendiendo el método de servicio:

recibir desde al menos una aplicación de las múltiples aplicaciones una petición de inicio de sesión que especifica un nombre de usuario y una contraseña introducidos por un usuario (U) del dispositivo (200) terminal cuando un testigo de acceso emitido a la aplicación (31, 32, 33) no está almacenado en una región de almacenamiento no volátil reservada para la aplicación (31, 32, 33) por el dispositivo (200) terminal, y

recibir desde al menos una aplicación de las múltiples aplicaciones, una petición de acceso que especifica el testigo de acceso emitido a la aplicación (31, 32, 33) cuando el testigo de acceso está almacenado en la región de almacenamiento no volátil, y el dispositivo (100) servidor,

realizar autenticación con el nombre de usuario y la contraseña especificados en la petición de inicio de sesión cuando se recibe la petición de inicio de sesión transmitida por cualquiera de las aplicaciones (31) que se ejecutan en el dispositivo (200) terminal,

emitir el testigo de acceso asociado con el nombre de usuario especificado en la petición de inicio de sesión a una aplicación (31) de fuente de transmisión que ha transmitido la petición de inicio de sesión si la autenticación es satisfactoria, transmitir el testigo de acceso emitido a la aplicación (31) de fuente de transmisión, y aprobar el acceso desde la aplicación (31) de fuente de transmisión,

almacenar el testigo de acceso emitido en asociación con un código de identificación de terminal que presenta el dispositivo (200) terminal en el que se ejecuta la aplicación (31) de fuente de transmisión que ha transmitido la petición de inicio de sesión y con la adición de una fecha de expiración, y posponer las fechas de expiración dadas a otros testigos de acceso almacenados en asociación con el código de identificación

de terminal, y

aprobar el acceso desde una aplicación (31) de fuente de transmisión que ha transmitido la petición de acceso y posponer las fechas de expiración dadas a todos los testigos de acceso almacenados en asociación con el código de identificación de terminal del dispositivo (200) terminal en el que se ejecuta la aplicación (31) de fuente de transmisión cuando se recibe la petición de acceso transmitida por cualquiera de las aplicaciones (31) que se ejecutan en el dispositivo (200) terminal y el testigo de acceso especificado en la petición de acceso está almacenado en asociación con el código de identificación de terminal y como no expirado.

9. Programa que comprende instrucciones que, cuando el programa se ejecuta por un ordenador que recibe acceso desde múltiples aplicaciones (31, 32, 33) que se ejecutan en un dispositivo (200) terminal, hacen que el ordenador lleve a cabo las etapas de:

recibir, desde al menos una aplicación de las múltiples aplicaciones una petición de inicio de sesión que especifica un nombre de usuario y una contraseña introducidos por un usuario (U) del dispositivo (200) terminal cuando un testigo de acceso emitido a la aplicación (31, 32, 33) no está almacenado en una región de almacenamiento no volátil reservada para la aplicación (31, 32, 33) por el dispositivo (200) terminal y

recibir, desde al menos una aplicación de las múltiples aplicaciones, una petición de acceso que especifica el testigo de acceso emitido a la aplicación (31, 32, 33) cuando el testigo de acceso está almacenado en la región de almacenamiento no volátil, y el dispositivo (100) servidor,

un procedimiento de autenticación de inicio de sesión para realizar autenticación con el nombre de usuario y la contraseña especificados en la petición de inicio de sesión cuando se recibe la petición de inicio de sesión transmitida por cualquiera de las aplicaciones (31) que se ejecutan en el dispositivo (200) terminal;

un procedimiento de aprobación para emitir el testigo de acceso asociado con el nombre de usuario especificado en la petición de inicio de sesión a una aplicación (31) de fuente de transmisión que ha transmitido la petición de inicio de sesión si la autenticación es satisfactoria, transmitir el testigo de acceso emitido a la aplicación (31) de fuente de transmisión, y aprobar el acceso desde la aplicación (31) de fuente de transmisión;

un primer procedimiento de ampliación para almacenar el testigo de acceso emitido en asociación con un código de identificación de terminal que presenta el dispositivo (200) terminal en el que se ejecuta la aplicación (31) de fuente de transmisión que ha transmitido la petición de inicio de sesión y con la adición de una fecha de expiración, y posponer las fechas de expiración dadas a otros testigos de acceso almacenados en asociación con el código de identificación de terminal;

un procedimiento de autenticación de petición de acceso para aprobar el acceso desde una aplicación (31) de fuente de transmisión que ha transmitido la petición de acceso cuando se recibe la petición de acceso transmitida por cualquiera de las aplicaciones (31) que se ejecutan en el dispositivo (200) terminal y el testigo de acceso especificado en la petición de acceso está almacenado en asociación con el código de identificación de terminal del dispositivo (200) terminal en el que se ejecuta la aplicación (31) de fuente de transmisión y como no expirado; y

un segundo procedimiento de ampliación para posponer las fechas de expiración dadas a todos los testigos de acceso almacenados en asociación con el código de identificación de terminal del dispositivo (200) terminal en el que se ejecuta la aplicación (31) de fuente de transmisión que ha transmitido la petición de acceso cuando el testigo de acceso especificado en la petición de acceso recibida está almacenado en asociación con el código de identificación de terminal y como no expirado.

FIG.1

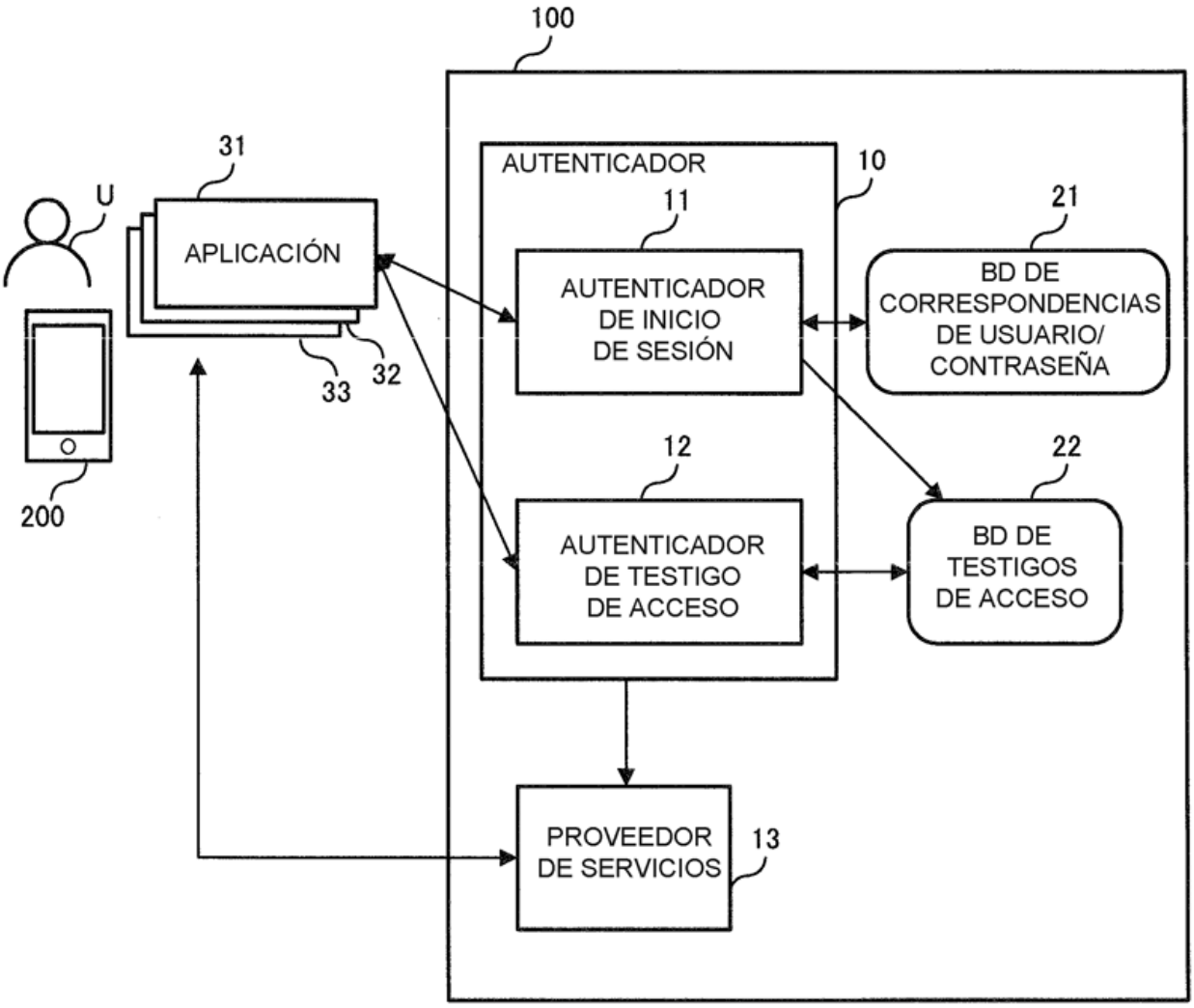

100
AUTENTICADOR
10
11
21
31
U
APLICACIÓN
AUTENTICADOR DE INICIO DE SESIÓN
BD DE CORRESPONDENCIAS DE USUARIO/ CONTRASEÑA
33
32
12
22
200
AUTENTICADOR DE TESTIGO DE ACCESO
BD DE TESTIGOS DE ACCESO
PROVEEDOR DE SERVICIOS
13

FIG.2

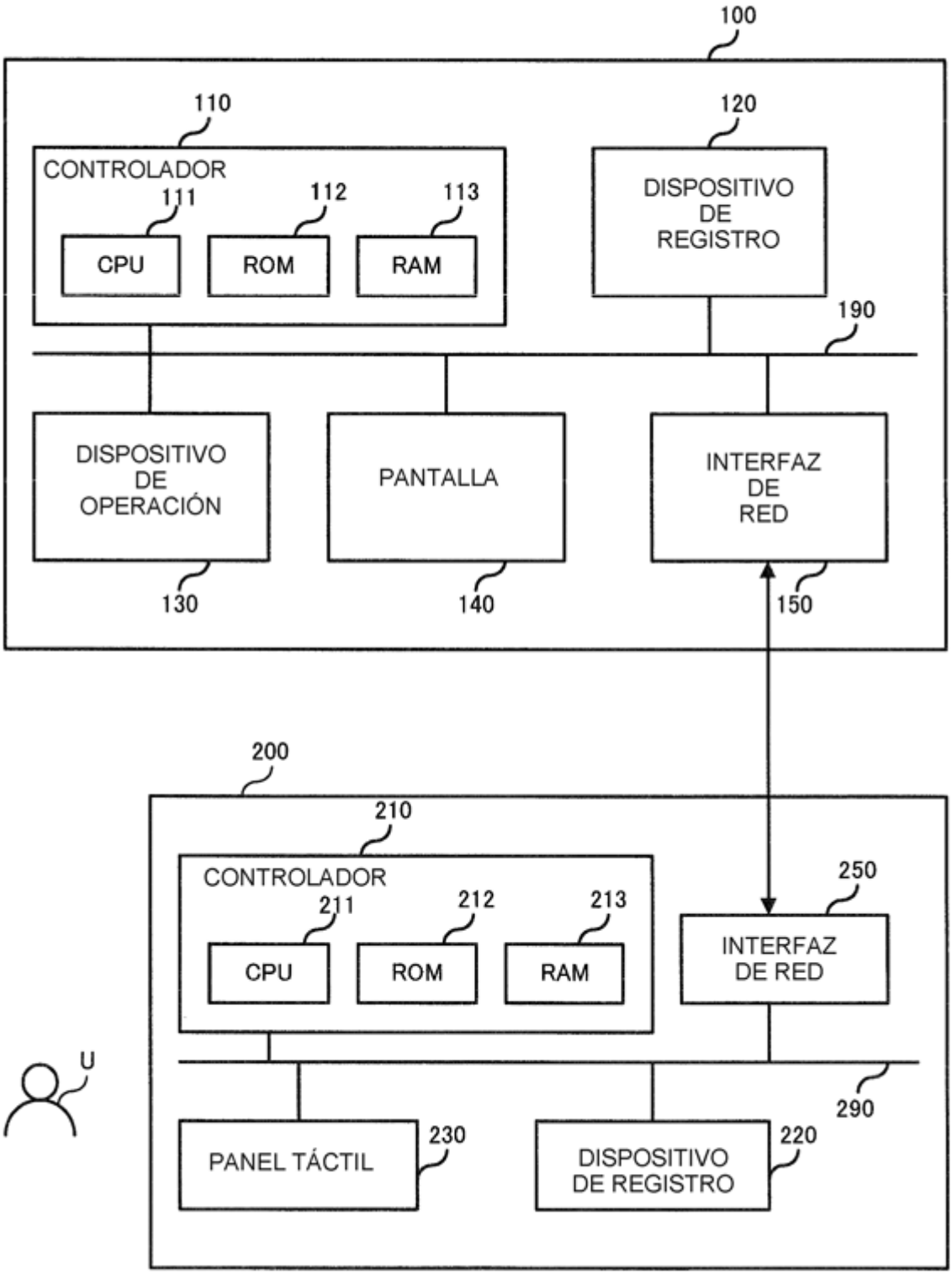

100
110
CONTROLADOR
111
112
113
CPU
ROM
RAM
120
DISPOSITIVO DE REGISTRO
190
DISPOSITIVO DE OPERACIÓN
PANTALLA
INTERFAZ DE RED
130
140
150
200
210
CONTROLADOR
211
212
213
CPU
ROM
RAM
250
INTERFAZ DE RED
U
290
PANEL TÁCTIL
230
DISPOSITIVO DE REGISTRO
220

FIG.3

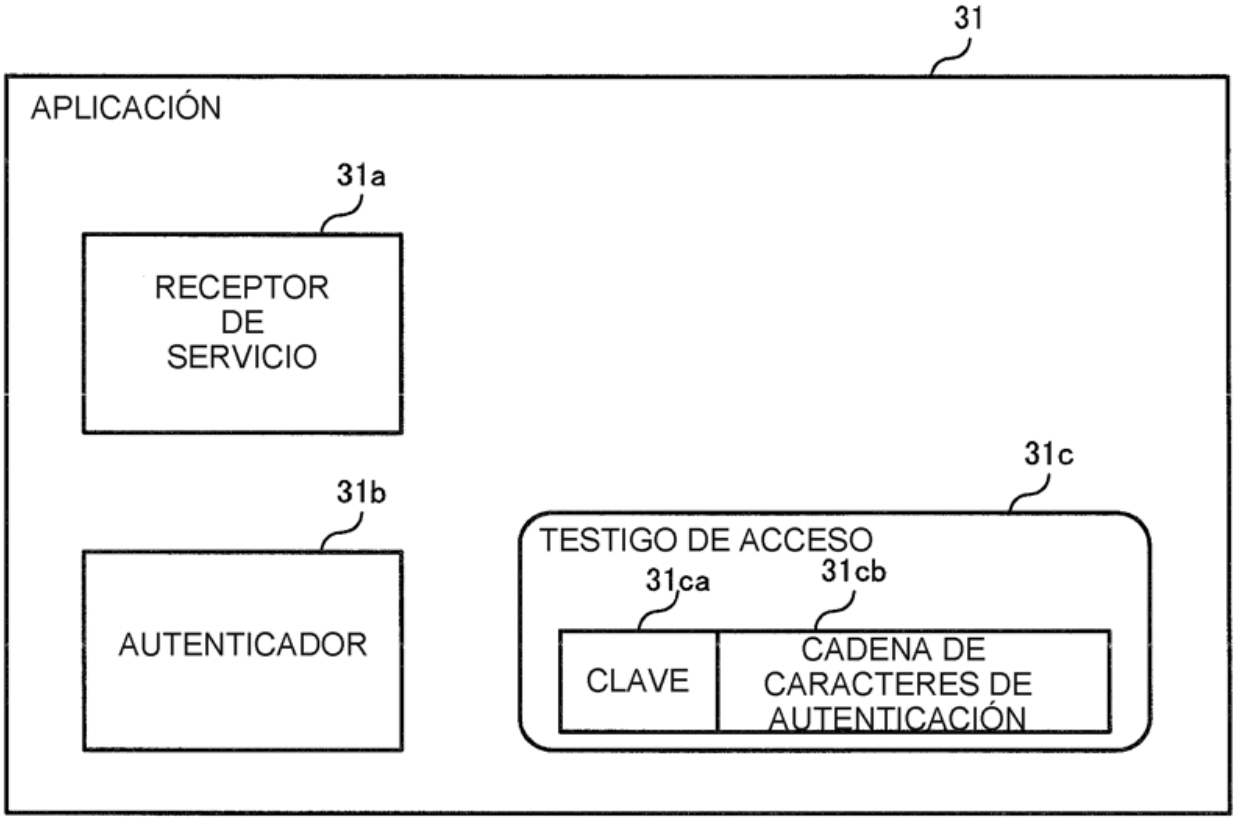

31
APLICACIÓN
31a
RECEPTOR DE SERVICIO
31b
AUTENTICADOR
31c
TESTIGO DE ACCESO
31ca
31cb
CLAVE
CADENA DE CARACTERES DE AUTENTICACIÓN

FIG.4

NOMBRE DE USUARIO	CONTRASEÑA
taro	ciud6be2d
usuario123	contraseña
hana	xns8r3dc

FIG.5

22

	TESTIGO DE ACCESO	ID DE APLICACIÓN	NOMBRE DE USUARIO	FECHA DE EXPIRACIÓN	CÓDIGO DE IDENTIFICACIÓN DE TERMINAL
20012	4d7aujemcu3x	502383716	taro	21.8.2016	2033419312
20013	vsr42ldcd6dl	823731793	usuario123	14.8.2016	2285482245
20014	x3kqynhgz58s	654019126	taro	2.9.2016	2033419312

FIG.6

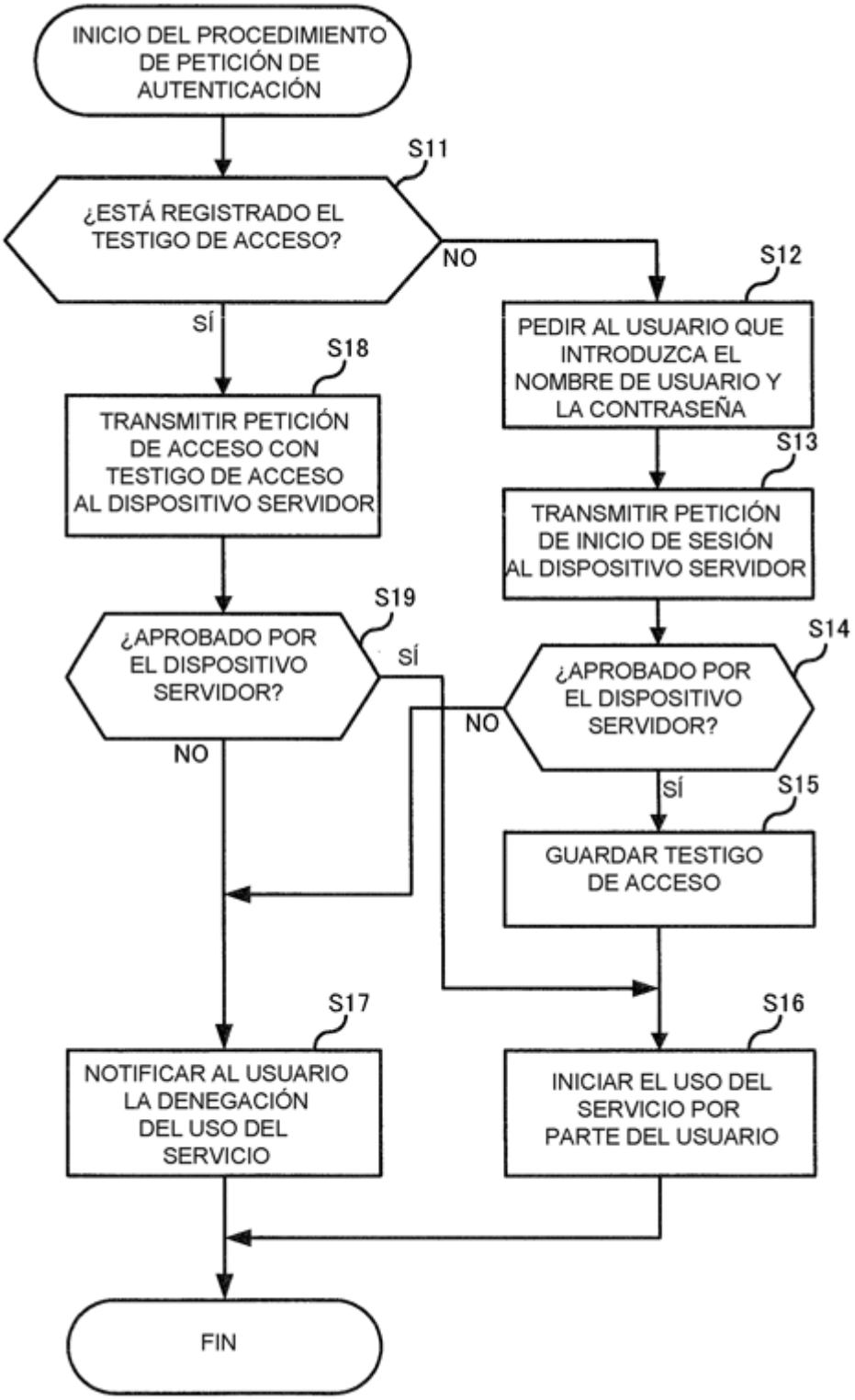

INICIO DEL PROCEDIMIENTO DE PETICIÓN DE AUTENTICACIÓN
S11
¿ESTÁ REGISTRADO EL TESTIGO DE ACCESO?
NO
SÍ
S12
PEDIR AL USUARIO QUE INTRODUZCA EL NOMBRE DE USUARIO Y LA CONTRASEÑA
S13
TRANSMITIR PETICIÓN DE INICIO DE SESIÓN AL DISPOSITIVO SERVIDOR
S14
¿APROBADO POR EL DISPOSITIVO SERVIDOR?
NO
SÍ
S15
GUARDAR TESTIGO DE ACCESO
S18
TRANSMITIR PETICIÓN DE ACCESO CON TESTIGO DE ACCESO AL DISPOSITIVO SERVIDOR
S19
¿APROBADO POR EL DISPOSITIVO SERVIDOR?
SÍ
NO
S16
INICIAR EL USO DEL SERVICIO POR PARTE DEL USUARIO
S17
NOTIFICAR AL USUARIO LA DENEGACIÓN DEL USO DEL SERVICIO
FIN

FIG.7

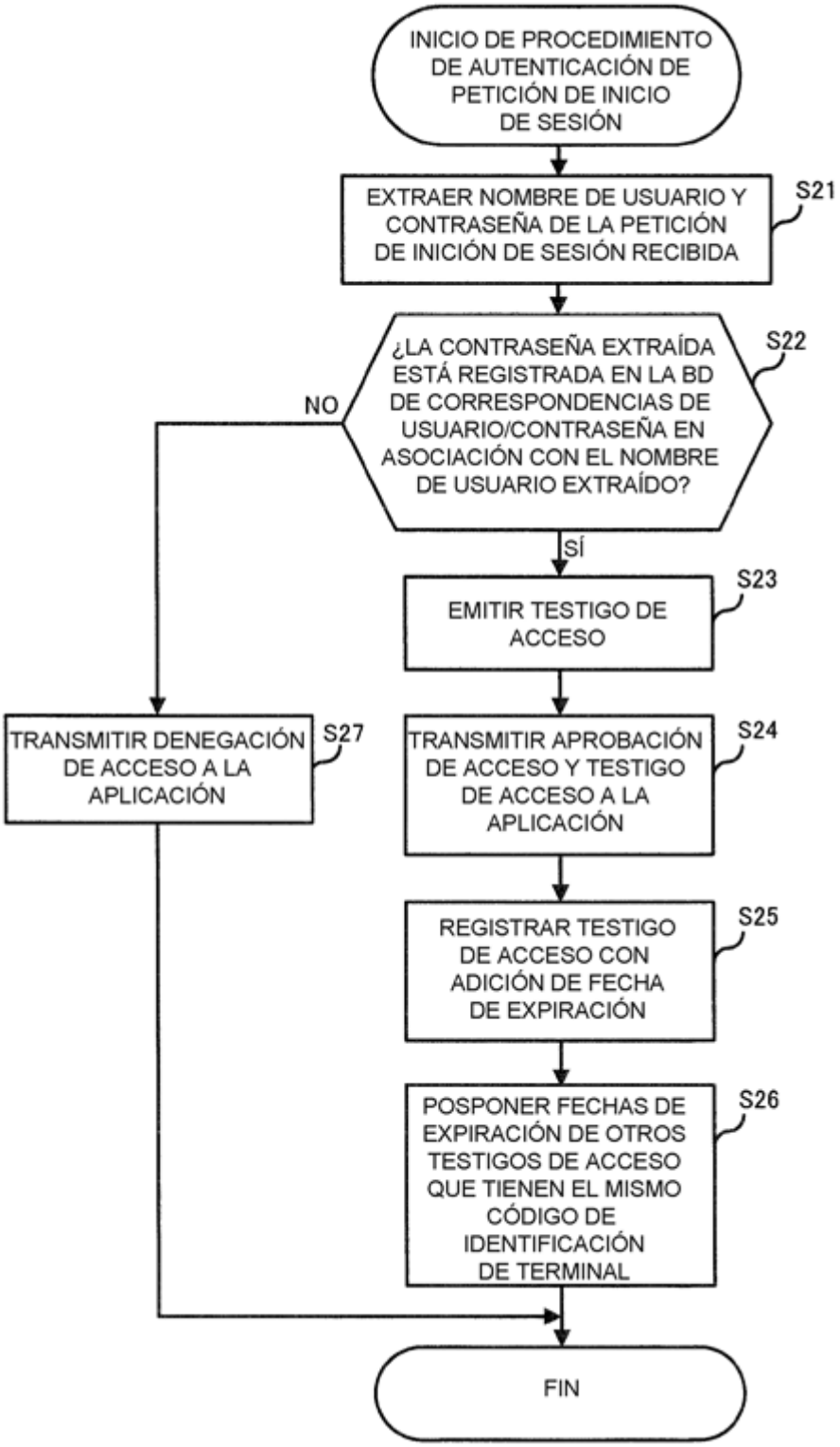
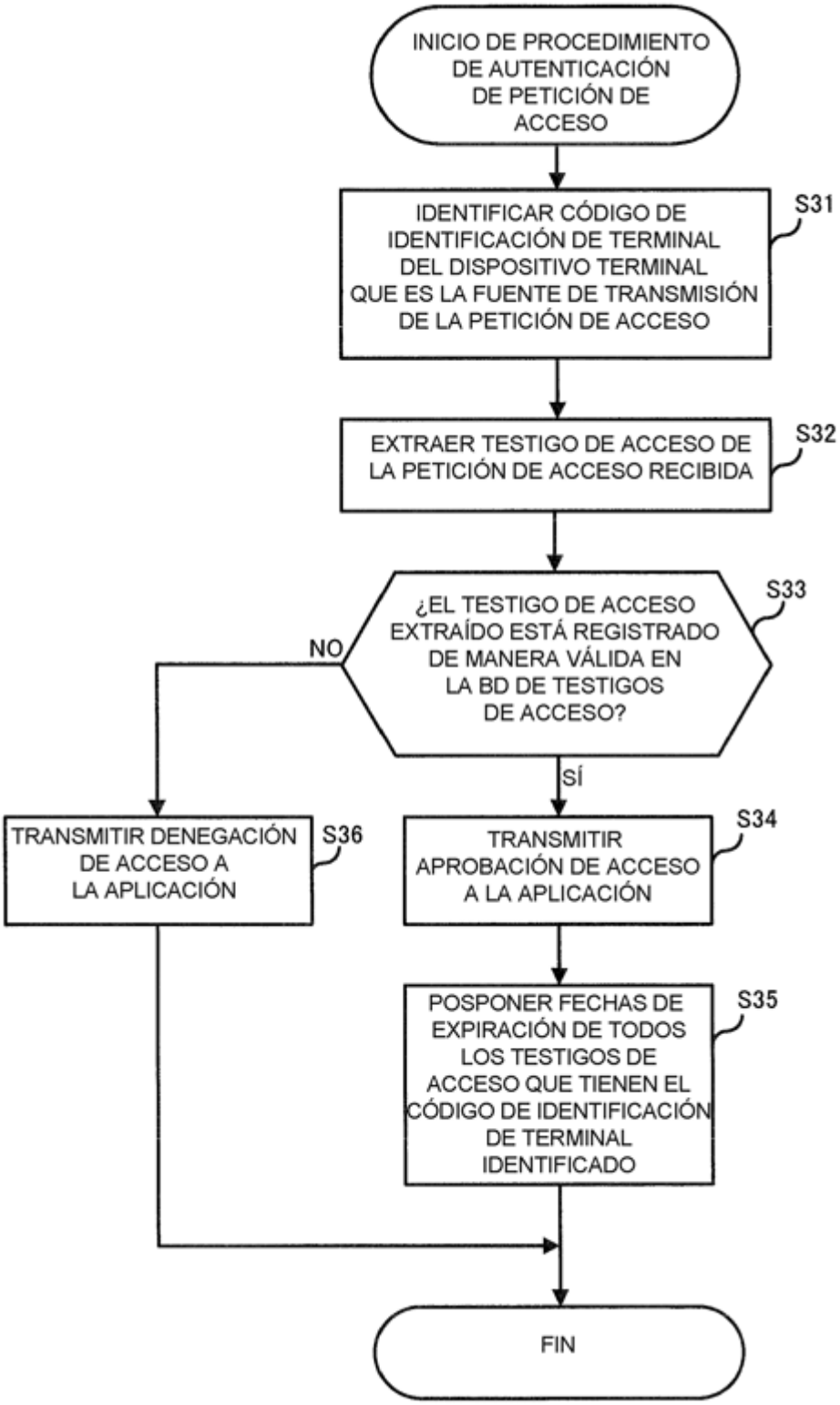

INICIO DE PROCEDIMIENTO DE AUTENTICACIÓN DE PETICIÓN DE INICIO DE SESIÓN
EXTRAER NOMBRE DE USUARIO Y CONTRASEÑA DE LA PETICIÓN DE INICIÓN DE SESIÓN RECIBIDA
S21
¿LA CONTRASEÑA EXTRAÍDA ESTÁ REGISTRADA EN LA BD DE CORRESPONDENCIAS DE USUARIO/CONTRASEÑA EN ASOCIACIÓN CON EL NOMBRE DE USUARIO EXTRAÍDO?
S22
NO
SÍ
EMITIR TESTIGO DE ACCESO
S23
TRANSMITIR DENEGACIÓN DE ACCESO A LA APLICACIÓN
S27
TRANSMITIR APROBACIÓN DE ACCESO Y TESTIGO DE ACCESO A LA APLICACIÓN
S24
REGISTRAR TESTIGO DE ACCESO CON ADICIÓN DE FECHA DE EXPIRACIÓN
S25
POSPONER FECHAS DE EXPIRACIÓN DE OTROS TESTIGOS DE ACCESO QUE TIENEN EL MISMO CÓDIGO DE IDENTIFICACIÓN DE TERMINAL
S26
FIN

FIG.8


INICIO DE PROCEDIMIENTO DE AUTENTICACIÓN DE PETICIÓN DE ACCESO
IDENTIFICAR CÓDIGO DE IDENTIFICACIÓN DE TERMINAL DEL DISPOSITIVO TERMINAL QUE ES LA FUENTE DE TRANSMISIÓN DE LA PETICIÓN DE ACCESO
S31
EXTRAER TESTIGO DE ACCESO DE LA PETICIÓN DE ACCESO RECIBIDA
S32
¿EL TESTIGO DE ACCESO EXTRAÍDO ESTÁ REGISTRADO DE MANERA VÁLIDA EN LA BD DE TESTIGOS DE ACCESO?
S33
NO
SÍ
TRANSMITIR DENEGACIÓN DE ACCESO A LA APLICACIÓN
S36
TRANSMITIR APROBACIÓN DE ACCESO A LA APLICACIÓN
S34
POSPONER FECHAS DE EXPIRACIÓN DE TODOS LOS TESTIGOS DE ACCESO QUE TIENEN EL CÓDIGO DE IDENTIFICACIÓN DE TERMINAL IDENTIFICADO
S35
FIN