(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 644 593**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
G06F 21/33 (2013.01)
G06F 17/30 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.06.2012 PCT/CN2012/077939**

(87) Fecha y número de publicación internacional: **03.01.2014 WO14000281**

(96) Fecha de presentación y número de la solicitud europea: **29.06.2012 E 12879738 (8)**

(97) Fecha y número de publicación de la concesión europea: **06.09.2017 EP 2860906**

(54) Título: **Método y dispositivo de autentificación de identidad**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.11.2017

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian Longgang District , Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

LI, LI y
HU, LIXIN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y dispositivo de autentificación de identidad.

Campo técnico

Las realizaciones de la presente invención se refieren a las técnicas de red y, en particular, a un método y un dispositivo para la autentificación de identidad.

Antecedentes

Una aplicación web (página web) es un programa de aplicación que se escribe utilizando un lenguaje admitido por el navegador y toma al navegador como entorno operativo y de presentación. Cuando un usuario utiliza una aplicación web, con el fin de garantizar la seguridad de uso de los recursos del sistema de red, habitualmente se necesita llevar a cabo una autentificación de identidad del usuario, de modo que un usuario legítimo acceda a los recursos del sistema de red con una autoridad legítima.

En la técnica anterior, en general, la autentificación de identidad de un usuario se lleva a cabo mediante la utilización de un nombre de usuario y una introducción de contraseña por parte del usuario, el usuario necesita recordar el nombre de usuario y la contraseña, además, la contraseña puede ser interceptada fácilmente por un tercero durante un proceso de transmisión, la seguridad no es alta, y la introducción de la contraseña es relativamente problemática y no lo suficiente práctica.

El documento CN 101610157 A describe un método para firmar de forma automática con un certificado digital en un formulario web. Un servidor de aplicación transmite el código de identificación único de un certificado digital seleccionado manualmente por el usuario por adelantado a una interfaz de usuario y un ActiveX de firma en el navegador local del usuario encuentra el certificado que es acorde con el código de identificación único transmitido por el servidor de aplicación de la lista de certificados digitales personal local, firma de forma automática el formulario, y envía la firma al servidor de aplicación.

El documento US 2008/0189778 A1 describe un método y un aparato para la autentificación de un cliente. En una realización, un servidor de proveedor de identidad autentifica al cliente que es redirigido desde un servidor de parte confiante. El servidor de proveedor de identidad autentifica al cliente sin recibir una credencial reproducible del cliente. Tras la autentificación del cliente, el servidor de proveedor de identidad transmite un token de autentificación al cliente.

Compendio

Las realizaciones de la presente invención proporcionan un método y un dispositivo para la autentificación de identidad, de manera que se mejore la practicidad y la seguridad de la autentificación de identidad.

Las realizaciones de la presente invención proporcionan un método para la autentificación de identidad, que incluye:

la detección, por una unidad de núcleo de navegador, de un evento de activación de inicio de sesión, y el envío del evento de activación de inicio de sesión a una unidad de aplicación web;

la determinación, por la unidad de aplicación web, de una dirección de sitio web correspondiente a una operación de activación de inicio de sesión en función del evento de activación de inicio de sesión, y el envío de la dirección de sitio web a la unidad de núcleo de navegador;

el envío, por la unidad de núcleo de navegador, de una petición de acceso a un servidor de aplicación en función de la dirección de sitio web enviada por la unidad de aplicación web; y

la recepción, por la unidad de núcleo de navegador, de una información de indicación que necesita la autentificación de identidad devuelta por el servidor de aplicación en función de la petición de acceso, en la que la información de indicación que necesita la autentificación de identidad lleva un parámetro de definición de autentificación de identidad, y la determinación de un certificado digital de usuario seleccionado que coincide con el parámetro de restricción de autentificación de identidad mediante la realización de una filtración de los certificados digitales de usuario en función del parámetro de definición de autentificación de identidad, en el que el parámetro de restricción de autentificación de identidad incluye uno cualquiera o más de una expedición de certificado, un tipo de certificado, un algoritmo de firma y un algoritmo de clave pública;

la generación, por una unidad de núcleo de navegador, de una petición de inicio de sesión que lleva un certificado digital de usuario seleccionado en función del certificado digital de usuario seleccionado, y el envío de la petición de inicio de sesión a un servidor de aplicación;

la recepción, por la unidad de núcleo de navegador, de una respuesta que indica el éxito de autentificación que es devuelta por el servidor de aplicación después de llevar a cabo la autentificación de identidad en función del certificado digital seleccionado, la extracción de un fichero de página web de la respuesta, el análisis sintáctico del fichero de página web, la generación de una página web y el envío de la página web a una unidad de interfaz de navegador; y;

la presentación visual, por la unidad de interfaz de navegador, de la página web.

Las realizaciones de la presente invención proporcionan un dispositivo para la autentificación de identidad, que incluye: una unidad de aplicación web, una unidad de núcleo de navegador y una unidad de interfaz de navegador;

la unidad de aplicación web está configurada para determinar una dirección de sitio web correspondiente a una operación de activación de inicio de sesión en función de un evento de activación de inicio de sesión, y enviar la dirección de sitio web a la unidad de núcleo de navegador;

la unidad de núcleo de navegador está configurada para detectar el evento de activación de inicio de sesión, enviar el evento de activación de inicio de sesión a la unidad de aplicación web, y enviar una petición de acceso al servidor de aplicación en función de una dirección de sitio web enviada por la unidad de aplicación web, recibir una información de indicación que necesita la autentificación de identidad devuelta por el servidor de aplicación en función de la petición de acceso, en donde la información de indicación que necesita la autentificación de identidad lleva un parámetro de definición de autentificación de identidad, y determinar un certificado digital de usuario seleccionado que coincide con el parámetro de restricción de autentificación de identidad mediante la realización de una verificación de los certificados digitales de usuario en función del parámetro de definición de autentificación de identidad, en donde el parámetro de restricción de autentificación de identidad incluye uno cualquiera o más de una expedición de certificado, un tipo de certificado, un algoritmo de firma y un algoritmo de clave pública, generar una petición de inicio de sesión que lleva un certificado digital de usuario seleccionado en función del certificado digital de usuario seleccionado, enviar la petición de inicio de sesión a un servidor de aplicación, recibir una respuesta que indica el éxito de autentificación que es devuelta por el servidor de aplicación después de llevar a cabo la autentificación de identidad en función del certificado digital seleccionado, extraer un fichero de página web de la respuesta, analizar sintácticamente el fichero de página web, generar una página web y enviar la página web a una unidad de interfaz de navegador;

la unidad de interfaz de navegador está configurada para presentar visualmente la página web.

Como se ve a partir de las soluciones técnicas anteriores, según el método de autentificación de identidad proporcionado por esta realización, una unidad de núcleo de navegador genera una petición de inicio de sesión que lleva un certificado digital de usuario seleccionado en función del certificado digital de usuario seleccionado, envía la petición de inicio de sesión a un servidor de aplicación; la unidad de núcleo de navegador recibe una respuesta para indicar el éxito de autentificación enviada por el servidor de aplicación, extrae un fichero de página web de la respuesta, analiza sintácticamente el fichero de página web, genera una página web y envía la página web a una unidad de interfaz de navegador; la unidad de interfaz de navegador presenta visualmente la página web. La autentificación de identidad se lleva a cabo mediante el certificado de usuario digital de usuario, un usuario no necesita recordar un nombre de usuario y una contraseña, evitando de esta manera la interceptación de la contraseña durante un proceso de transmisión, y mejorando la practicidad y la seguridad de la autentificación de identidad.

Breve descripción de los dibujos

Con el fin de hacer las soluciones técnicas en las realizaciones de la presente invención o en la técnica anterior de forma más clara, los dibujos adjuntos utilizados en la descripción de las realizaciones o la técnica anterior se describirán de forma breve a continuación. Como es obvio, los dibujos descritos son meramente algunas realizaciones de la presente invención. Para las personas expertas en la técnica, se pueden obtener otros dibujos en base a estos dibujos sin ningún esfuerzo creativo.

La Figura 1 es un diagrama de flujo de un primer método para la autentificación de identidad según una realización de la presente invención;

la Figura 2 es un diagrama de flujo de un segundo método para la autentificación de identidad según una realización de la presente invención;

la Figura 3 es un diagrama de flujo de un método para la implementación de la etapa 204 como se muestra en la Figura 2 según una realización de la presente invención;

la Figura 4 es un diagrama de señalización de una autentificación de identidad según una realización de la presente invención;

la Figura 5 es un diagrama de flujo de un tercer método para la autentificación de identidad según una realización de la presente invención;

la Figura 6 es un diagrama de señalización de otra autentificación de identidad según una realización de la presente invención;

la Figura 7 es un diagrama de flujo de un cuarto método para la autentificación de identidad según una realización de la presente invención;

la Figura 8 es un diagrama de señalización de incluso otra autentificación de identidad según una realización de la presente invención;

la Figura 9 es un diagrama de flujo de un quinto método para la autentificación de identidad según una realización de la presente invención;

la Figura 10 es un diagrama estructural esquemático de un sistema para la autentificación de identidad según una realización de la presente invención;

la Figura 11 es un diagrama estructural esquemático de otro sistema para la autentificación de identidad según una realización de la presente invención.

Descripción de las realizaciones

Con el fin de hacer los objetivos, soluciones técnicas y ventajas de las realizaciones de la presente invención de forma más clara, las soluciones técnicas en las realizaciones de la presente invención se describen en lo sucesivo de forma clara y completa con referencia a los dibujos adjuntos en las realizaciones de la presente invención. Como es obvio, las realizaciones descritas son solo una parte de las realizaciones de la presente invención, en lugar de todas las realizaciones de la presente invención. Todas las demás realizaciones obtenidas por personas con experiencia ordinaria en la técnica en base a las realizaciones de la presente invención sin ningún esfuerzo creativo entrarán dentro del alcance de protección de la presente invención.

La Figura 1 es un diagrama de flujo de un primer método para la autentificación de identidad según una realización de la presente invención. Como se muestra en la Figura 1, el método para la autentificación de identidad según esta realización de la presente invención se puede aplicar específicamente a un proceso de autentificación de identidad de usuario cuando el usuario utiliza una aplicación web a través de un navegador, y se puede ejecutar por medio de un dispositivo para la autentificación de identidad provisto de un navegador. El dispositivo para la autentificación de identidad puede ser un dispositivo tal como un ordenador personal, un portátil, un ordenador de pantalla plana y un smartphone.

El método para la autentificación de identidad según esta realización incluye específicamente:

la etapa 101, la generación, por una unidad de núcleo de navegador, de una petición de inicio de sesión que lleva un certificado digital de usuario seleccionado en función del certificado digital de usuario seleccionado, y el envío de la petición de inicio de sesión a un servidor de aplicación;

la etapa 102, la recepción, por la unidad de núcleo de navegador, de una respuesta que indica el éxito de autentificación que es devuelta por el servidor de aplicación después de llevar a cabo la autentificación de identidad en función del certificado digital seleccionado, la extracción de un fichero de página web de la respuesta, el análisis sintáctico del fichero de la página web, la generación de una página web y el envío de la página web a una unidad de interfaz de navegador; y

la etapa 103, la presentación visual, por la unidad de interfaz de navegador, de la página web.

Específicamente, un usuario se registra para ser un usuario legítimo de una aplicación web en primer lugar, la aplicación web distribuye un certificado digital de usuario correspondiente a un cliente del usuario, en el que el mismo se almacena en un dispositivo de autentificación de identidad. Específicamente, el certificado digital de usuario puede utilizar un sistema de clave pública, es decir, utilizar un par de claves que coinciden entre sí para el cifrado y el descifrado. Durante un proceso de transmisión de red, solo se transmitirá una clave pública, y una clave privada se almacena solamente de forma local en el usuario. Por consiguiente, incluso si el certificado digital de usuario es interceptado, el certificado digital de usuario no será descifrado y no se pueden adquirir los datos reales del certificado digital de usuario. Cuando el usuario lleva a cabo el registro a través de una pluralidad de identidades de usuario, cada una de las identidades de usuario tendrá su propio certificado digital de usuario correspondiente, en el que una WebID (una identidad de un usuario en una página web) puede ser utilizada para identificar la identidad de usuario para conseguir la unicidad de la identidad de usuario. El certificado digital de usuario puede incluir información tal como una WebID, un emisor de certificado, un tipo de certificado, una clave pública de certificado y un algoritmo de firma digital. Cuando un usuario necesita iniciar sesión con una identidad de usuario determinada, se

puede seleccionar un certificado digital de usuario correspondiente a la identidad de usuario, en este momento, el certificado digital de usuario correspondiente a la identidad de usuario seleccionada por el usuario es concretamente el certificado digital de usuario seleccionado.

La unidad de núcleo de navegador está específicamente provista de un programa de núcleo de navegador, la unidad de núcleo de navegador genera una petición de inicio de sesión que lleva el certificado digital de usuario seleccionado en función del certificado digital de usuario seleccionado, la petición de inicio de sesión se utiliza para indicar una petición para llevar a cabo un procesamiento de inicio de sesión para la identidad de usuario correspondiente al certificado digital de usuario, donde la petición de inicio de sesión es específicamente una petición GET (get, obtención) HTTP (HyperText Transfer Protocol, Protocolo de Transferencia de Hipertexto). La unidad de núcleo de navegador envía la petición de inicio de sesión a un servidor de aplicación correspondiente a la aplicación web, en el que el servidor de aplicación recibe la petición de inicio de sesión y valida el certificado digital de usuario en la petición de inicio de sesión.

Específicamente, el método para la validación del certificado digital de usuario por el servidor de aplicación puede incluir los dos tipos siguientes:

un método de implementación: el servidor de aplicación puede iniciar una petición de consulta a un servidor de autentificación correspondiente mediante una manera de SPARQL (Simple Protocol and RDF Query Language, Protocolo Simple y Lenguaje de Consulta RDF), donde la petición de consulta puede llevar varios parámetros de clave en el certificado digital de usuario, por ejemplo, una WebID, un tipo de certificado, una clave pública de certificado, etc., el servidor de autentificación lleva a cabo una consulta en función de los varios parámetros de clave anteriores; cuando los parámetros de un certificado digital de usuario determinado almacenado en el servidor de autentificación son todos iguales con respecto a los varios parámetros de clave llevados durante el proceso de consulta anterior, entonces el resultado de consulta es verdadero, la autentificación de identidad se realiza correctamente; cuando los parámetros de un certificado digital de usuario determinado almacenado en el servidor de autentificación son totalmente diferentes de o no son completamente iguales con respecto a los varios parámetros de clave llevados durante el proceso de consulta anterior, la autentificación de identidad falla.

El otro método de implementación: el servidor de aplicación adquiere un certificado digital de usuario correspondiente a la WebID almacenado/a en el servidor de autentificación mediante una petición GET HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, Protocolo de Transferencia de Hipertexto por Capa de Conexión Segura, un mensaje HTTP que se transmite de forma segura). El servidor de aplicación hace coincidir un certificado digital de usuario llevado en una petición de inicio de sesión recibida con el certificado digital de usuario adquirido del servidor de autentificación, si los parámetros de los dos certificados digitales de usuario son todos iguales, es decir, la coincidencia se realiza correctamente, entonces la autentificación de identidad de usuario se realiza correctamente, si los parámetros de los dos certificados digitales de usuario son totalmente diferentes o no son completamente iguales, entonces la autentificación de identidad falla.

Si la autentificación de identidad de usuario tiene éxito, entonces se envía una respuesta para indicar el éxito de autentificación a la unidad de núcleo de navegador, donde la respuesta lleva un fichero de web correspondiente a la aplicación web, y la respuesta que indica el éxito de autentificación puede ser específicamente una respuesta de HTTP 200. La unidad de núcleo de navegador extrae un fichero de web de la respuesta, analiza sintácticamente el fichero de web, ejecuta el fichero de web, lleva a cabo una representación correspondiente y presenta visualmente la página web final mediante una unidad de interfaz de navegador, para proporcionar una aplicación web correspondiente al usuario. El fichero de página web puede incluir específicamente un fichero de Lenguaje de Marcado de Hipertexto (Hypertext Markup Language, de forma abreviada, HTML), un fichero de comandos javascript y un fichero de Hoja de Estilo en Cascada (Cascading Style Sheet, de forma abreviada, CSS), etc. La unidad de interfaz de navegador está provista de un programa de interfaz de navegador. Cuando la autentificación de identidad de usuario falla, el servidor de aplicación también devuelve una respuesta para indicar el fallo de autentificación a la unidad de núcleo de navegador, donde la respuesta que indica el fallo de autentificación puede ser específicamente una respuesta HTTP 403.

Según el método de autentificación de identidad proporcionado por esta realización, una unidad de núcleo de navegador genera una petición de inicio de sesión que lleva un certificado digital de usuario seleccionado en función del certificado digital de usuario seleccionado, envía la petición de inicio de sesión a un servidor de aplicación; la unidad de núcleo de navegador recibe una respuesta para indicar el éxito de autentificación enviada por el servidor de aplicación, extrae un fichero de página web de la respuesta, analiza sintácticamente el fichero de página web, genera una página web y envía la página web a una unidad de interfaz de navegador; la unidad de interfaz de navegador presenta visualmente la página web. La autentificación de identidad se lleva a cabo mediante el certificado de usuario digital de usuario, un usuario no necesita recordar un nombre de usuario y una contraseña, evitando de esta manera la interceptación de la contraseña durante un proceso de transmisión y mejorando la practicidad y la seguridad de la autentificación de identidad.

La Figura 2 es un diagrama de flujo de un segundo método para la autentificación de identidad según una realización de la presente invención. Como se muestra en la Figura 2, en esta realización, en la Etapa 101 de la realización como se muestra en la Figura 1, antes de la generación, por la unidad de núcleo de navegador, de la petición de inicio de sesión que lleva el certificado digital de usuario seleccionado en función del certificado digital de usuario seleccionado, el método puede incluir además las siguientes etapas:

etapa 201, la detección, por la unidad de núcleo de navegador, de un evento de activación de inicio de sesión, y el envío del evento de activación de inicio de sesión a una unidad de aplicación web;

etapa 202, la determinación, por la unidad de aplicación web, de una dirección de sitio web correspondiente a una operación de activación de inicio de sesión en función del evento de activación de inicio de sesión, y el envío de la dirección de sitio web a la unidad de núcleo de navegador;

etapa 203, el envío, por la unidad de núcleo de navegador, de una petición de acceso al servidor de aplicación en función de la dirección de sitio web enviada por la unidad de aplicación web;

etapa 204, la recepción, por la unidad de núcleo de navegador, de la información que necesita la autentificación de identidad devuelta por el servidor de aplicación en función de la petición de acceso, y la determinación del certificado digital de usuario seleccionado en función de la información de indicación que necesita la autentificación de identidad. Específicamente, la unidad de aplicación web está provista de una aplicación web. En un escenario de aplicación, cuando un usuario utiliza la aplicación web mediante un navegador, si los recursos de red a los que se accede no necesitan autentificación de identidad, el usuario no necesita iniciar sesión. Si los recursos de red a los que accede el usuario necesitan autentificación de identidad, entonces es necesario que el usuario proporcione un certificado digital de usuario, para llevar a cabo la autentificación de identidad.

El evento de activación de inicio de sesión es específicamente un evento que activa una operación de inicio de sesión, por ejemplo, cuando el usuario hace clic en un texto, un botón o una imagen que incluye un hipervínculo en la página web presentada visualmente por la unidad de interfaz de navegador, se generará un evento de clic de usuario, en el que el evento de clic que lleva específicamente una identificación del texto, un botón o una imagen en los que hace clic el usuario, la unidad de interfaz de navegador notifica el evento de clic de usuario a la unidad de núcleo de navegador, el evento de clic de usuario puede servir como el evento de activación de inicio de sesión, en este momento, la operación de inicio de sesión de activación puede ser una operación de clic, la dirección de sitio web correspondiente a la operación de inicio de sesión de activación puede ser la dirección de sitio web vinculada a la operación de clic. El evento de activación de inicio de sesión también puede ser una redirección de forma automática de página web, una reproducción de un vídeo hasta una duración determinada o una realización de una operación de copia por un usuario, etc. Cuando la unidad de núcleo de navegador detecta el evento de activación de inicio de sesión, la unidad de núcleo de navegador envía el evento de activación de inicio de sesión a la unidad de aplicación web. La unidad de aplicación web determina una dirección de sitio web correspondiente a la operación de activación de inicio de sesión en función del evento de activación de inicio de sesión, y envía la dirección de sitio web a la unidad de núcleo de navegador, la unidad de núcleo de navegador genera una petición de acceso que lleva la dirección de sitio web y envía la petición de acceso al servidor de aplicación. La petición de acceso puede ser específicamente una petición GET HTTP. El servidor de aplicación determina la seguridad, importancia y privacidad de los recursos de red a los que accede el usuario en función de la petición de acceso, si se considera que los recursos de red a los que el usuario pide acceder necesitan la autentificación de identidad del usuario, entonces envía la información de indicación que necesita la autentificación de identidad a la unidad de núcleo de navegador. La unidad de núcleo de navegador determina el certificado digital de usuario seleccionado en función de la información de indicación que necesita la autentificación de identidad.

La información de indicación que necesita la autentificación de identidad también puede llevar un parámetro de definición de autentificación de identidad, en el que el parámetro de restricción de autentificación de identidad puede incluir lo siguiente:

Emisor: una autoridad emisora, es decir, un emisor de certificado;

Tipos_certificados: un tipo de certificado, que puede ser una clave RSA (algoritmo de cifrado de clave pública RSA), una clave DSA (clave de algoritmo de firma digital, algoritmo de cifrado de clave pública DSA), una clave DH estático RSA (algoritmo de cifrado de clave pública de Diffie-Hellman estático RSA) o una clave DH estático DSA (algoritmo de cifrado de clave pública de Diffie-Hellman estático DSA);

Algoritmo de Firma: un algoritmo de firma;

Algoritmo de Clave Pública: un algoritmo de clave pública.

La unidad de núcleo de navegador puede llevar a cabo una filtración de los certificados digitales de usuario en función del parámetro de restricción de autentificación de identidad, para determinar un certificado digital de usuario que coincide con el parámetro de restricción de autentificación de identidad.

La Figura 3 es un diagrama de flujo de un método para la implementación de la etapa 204 como se muestra en la Figura 2. Como se muestra en la Figura 3, en esta realización, en la etapa 204 de la realización como se muestra en la Figura 2, la recepción, por la unidad de núcleo de navegador, de la información de indicación que necesita la autentificación de identidad devuelta por el servidor de aplicación en función de la petición de acceso, y la determinación del certificado digital de usuario seleccionado en función de la información de indicación que necesita la autentificación de identidad, puede incluir específicamente las siguientes etapas, como se muestra en la Figura 3:

etapa 2041, la generación, por la unidad de núcleo de navegador, de un evento que necesita la autentificación de identidad en función de la información de indicación que necesita la autentificación de identidad, y la notificación del evento que necesita la autentificación de identidad a la unidad de aplicación web;

etapa 2042, la recepción, por la unidad de aplicación web, del evento que necesita la autentificación de identidad y la invocación de una interfaz de inicio de sesión de un objeto de autentificación de la unidad de núcleo de navegador;

etapa 2043, la adquisición, por la unidad de núcleo de navegador, de un certificado digital de usuario predeterminado que se almacena localmente, y la determinación del certificado digital de usuario predeterminado como el certificado digital de usuario seleccionado, o la adquisición, por la unidad de núcleo de navegador, de una pluralidad de certificados digitales de usuario que se van a seleccionar que se almacenan localmente, y la determinación de un certificado digital de usuario de la pluralidad de certificados digitales de usuario que se van a seleccionar como el certificado digital de usuario seleccionado en función de la información de indicación de selección recibida.

Específicamente, la anterior información de indicación que necesita la autentificación de identidad puede ser específicamente una petición de protocolo de seguridad de capa de transporte (Transport Layer Security, de forma abreviada, TLS), la unidad de núcleo de navegador recibe la información de indicación que necesita la autentificación de identidad; si la información de indicación que necesita la autentificación de identidad lleva el parámetro de restricción de autentificación de identidad, entonces analiza sintácticamente el parámetro de restricción de autentificación de identidad de la información de indicación que necesita la autentificación de identidad. Comprobar si la unidad de aplicación web ha preestablecido una supervisión para el evento de autentificación de identidad de usuario; si es así, la unidad de núcleo de navegador notifica el evento que necesita la autentificación de identidad a la unidad de aplicación web, en la que el evento que necesita la autentificación de identidad puede llevar el parámetro de restricción de autentificación de identidad.

La unidad de aplicación web recibe el evento que necesita la autentificación de identidad y determina que es necesario llevar a cabo la autentificación de identidad del usuario. Considera si un objeto de ventana en un DOM de navegador (Document Object Model, Modelo de Objetos del Documento) incluye un subobjeto de función de inicio de sesión, en el que el subobjeto de función de inicio de sesión puede ser específicamente una Autentificación de WebID, si se detecta la ventana. AutentificaciónWebID, invoca una interfaz de inicio de sesión proporcionada por el objeto de autentificación en la unidad de núcleo de navegador, en la que el objeto de autentificación puede ser específicamente un objeto de AutentificaciónWebID, si no se crea el objeto de autentificación, el objeto de autentificación se puede crear en primer lugar, y la interfaz de inicio de sesión es específicamente una interfaz InicioSesión. Si el parámetro de restricción de autentificación de identidad existe, entonces el parámetro de restricción de autentificación de identidad se puede tomar como un parámetro y se transfiere a la unidad de núcleo de navegador mediante la interfaz de inicio de sesión. La unidad de aplicación web también puede detectar si la autentificación de identidad del usuario es necesaria en función de una lógica interna de aplicación web.

La interfaz InicioSesión se puede implementar específicamente a través de las siguientes funciones de interfaz:

interfaz AutentificaciónWebID : ObjetivoEvento {

atributo DOMCadena webID;//webID de usuario

sololectura [CD] atributo ListaCD;// lista de certificados digitales correspondiente a la webID

vacío InicioSesión(ContextoAutent contexto);//interfaz de autentificación de identidad de usuario

vacío CierreSesión(DOMCadena webID);//interfaz de cierre de sesión de usuario

vacío ConsultaEstadoUsuario(DOMCadena webID);//interfaz de consulta de estado de inicio de sesión de usuario //interfaz de llamada de respuesta

vacío atributo Función? InicioSesiónActivado;//interfaz de llamada de respuesta de autentificación de identidad de usuario

vacío atributo Función? CierreSesiónActivado; //interfaz de llamada de respuesta de cierre de sesión de usuario

vacío atributo Función? ActivadaConsultaEstadoUsuario;//interfaz de llamada de respuesta de consulta de estado de inicio de sesión de usuario };

Cuando la invocación de interfaz AutentificaciónWebID::InicioSesión es recibida por la unidad de núcleo de navegador, en función de una configuración de usuario o política de sistema predeterminadas, la unidad de núcleo de navegador detecta si la unidad de núcleo de navegador necesita seleccionar automáticamente un certificado digital de usuario determinado para el usuario para esta autentificación de identidad. El proceso de configuración de usuario puede ser específicamente: la selección de forma automática, por la unidad de núcleo de navegador, de un certificado digital de usuario preestablecido para el usuario, o el recordatorio al usuario de realizar una selección manualmente, cuando la unidad de núcleo de navegador necesita el certificado digital de usuario para llevar a cabo la autentificación de identidad en función de la configuración de usuario. Cuando la configuración no se lleva a cabo por el usuario, la unidad de núcleo de navegador puede llevar a cabo una operación en función de la política de sistema, por ejemplo, cuando solo hay un certificado digital de usuario almacenado localmente, la unidad de núcleo de navegador toma al certificado digital de usuario como un certificado digital de usuario predeterminado y lleva a cabo la autentificación de identidad, cuando hay una pluralidad de certificados digitales de usuario almacenados localmente, la unidad de núcleo de navegador presenta visualmente todos los certificados digitales de usuario al usuario, para facilitar que el usuario realice la selección.

Si es necesario llevar a cabo una selección automática, la unidad de núcleo de navegador adquiere un certificado digital de usuario predeterminado, si el parámetro de restricción de autentificación de identidad se transfiere cuando se invoca la interfaz InicioSesión, entonces también puede comprobar si el certificado digital de usuario predeterminado cumple el requisito del parámetro de restricción de autentificación de identidad. Mediante la confirmación de la utilización del certificado digital de usuario predeterminado para llevar a cabo esta autentificación de identidad, ya no es necesario llevar a cabo una interacción explícita con el usuario a través de una interfaz de gestor de certificados digitales, que puede acortar el tiempo de procesamiento para el proceso global en gran medida, y mejorar la eficiencia de procesamiento.

Si no es necesario llevar a cabo una selección automática, la unidad de núcleo de navegador adquiere la pluralidad de certificados digitales de usuario que se van a seleccionar para formar una lista de certificados digitales de usuario. Si el parámetro de restricción de autentificación de identidad se transfiere, también se les puede realizar una comprobación y una verificación de todos los certificados digitales de usuario gestionados en función del parámetro de restricción de autentificación de identidad, y se obtiene una lista de certificados digitales de usuario disponibles. Y la interfaz de gestor de certificados digitales emerge, la cual enumera todos los certificados digitales de usuario disponibles y provoca que el usuario seleccione un certificado digital de usuario determinado para la autentificación de identidad de este acceso de sitio web de los certificados digitales de usuario disponibles. Este método de procesamiento puede facilitar que el usuario realice inicios de sesión en diferentes aplicaciones web mediante la utilización de diferentes identidades de usuario.

Durante el proceso de implementación específico, la anterior interfaz de gestor de certificados digitales puede ser una interfaz de operación del gestor de certificados digitales implementado en la unidad de núcleo de navegador, si la unidad de núcleo de navegador implementa el gestor de certificados digitales por sí misma, la unidad de núcleo de navegador necesita leer un certificado digital almacenado por el equipo local y presentar visualmente el certificado digital en la interfaz de gestor de certificados digitales a través de una interfaz CAPICOM (Cryptographic API Component Object Model, Modelo de Objeto Componente API de Cifrado) proporcionada por el sistema operativo, en este método de implementación, el navegador puede llevar a cabo la lectura del certificado digital de usuario cuando se está iniciando, y también puede activar la lectura del certificado digital de usuario cuando procesa una aplicación y una página específicas, para proporcionar una eficiencia de procesamiento mayor. El gestor de certificados digitales también puede ser un gestor de certificados digitales proporcionado por el sistema operativo.

Si la unidad de aplicación web preestablece una supervisión para un evento de selección de certificado digital de usuario, la unidad de núcleo de navegador notifica el evento de selección de certificado digital a la aplicación web y transfiere el certificado digital de usuario seleccionado por el usuario como un parámetro a una capa de aplicación web mediante una interfaz de notificación de evento de selección de certificado digital. La unidad de aplicación web da instrucciones a la unidad de núcleo de navegador de que envíe la petición de inicio de sesión al servidor de aplicación.

La etapa 205 se lleva a cabo después de la etapa 204, la generación, por la unidad de núcleo de navegador y en función del certificado digital de usuario seleccionado, de la petición de inicio de sesión que lleva el certificado digital de usuario seleccionado, y el envío de la petición de inicio de sesión al servidor de aplicación;

etapa 206, la recepción, por la unidad de núcleo de navegador, de una respuesta que indica el éxito de autentificación que es devuelto por el servidor de aplicación después de llevar a cabo la autentificación de identidad en función del certificado digital seleccionado, la extracción del fichero de página web de la respuesta, el análisis sintáctico el fichero de página web, la generación de la página web y el envío de la página web a la unidad de interfaz de navegador;

etapa 207, la presentación visual, por la unidad de interfaz de navegador, de la página web.

Para la implementación específica de las etapas 205-207 de esta realización, se puede hacer referencia a las descripciones pertinentes de las etapas 101-103 de la realización como se muestra en la Figura 1.

En la etapa 206 de esta realización, después de la recepción, por la unidad de núcleo de navegador, de la respuesta que indica el éxito de autentificación que es devuelta por el servidor de aplicación después de llevar a cabo la autentificación de identidad en función del certificado digital seleccionado, y antes de la extracción, por la unidad de núcleo de navegador, del fichero de página web de la respuesta, el método incluye además: el análisis sintáctico, por la unidad de núcleo de navegador, un resultado de autentificación que indica el éxito de autentificación de la respuesta, y el envío del resultado de autentificación a la unidad de aplicación web mediante un evento de resultado de autentificación o una función de llamada de respuesta.

La unidad de núcleo de navegador analiza sintácticamente el resultado de autentificación que indica el éxito de autentificación de la respuesta y transfiere el resultado de autentificación a la unidad de aplicación web mediante la manera de notificación de un evento de resultado de autentificación o de invocación de una función de llamada de respuesta. Si la unidad de aplicación web preestablece una supervisión para el evento de resultado de autentificación, la unidad de núcleo de navegador notifica a la unidad de aplicación web del resultado de autentificación mediante la manera de notificación del evento de resultado de autentificación, no es necesario transferir una dirección de función y, de este modo, la eficiencia de operación es mayor. Si la unidad de aplicación web preimplementa una interfaz de llamada de respuesta InicioSesiónActivado, la unidad de núcleo de navegador puede transferir el resultado de autentificación a la unidad de aplicación web mediante la manera de invocación de la función de llamada de respuesta InicioSesiónActivado.

Ciertamente, el proceso específico de la etapa 207 es similar a la etapa 103 de la realización como se muestra en la Figura 1, es decir, para la implementación específica de la etapa 103, se puede hacer referencia a la etapa 207.

La Figura 4 es un diagrama de una autentificación de identidad según una realización de la presente invención. El método para la autentificación de identidad según esta realización se ilustrará en detalle a continuación con referencia a la Figura 4.

401, un usuario hace clic en un texto, un botón o una imagen que incluye un hipervínculo en una página web presentada visualmente por una unidad de interfaz de navegador;

402, la unidad de interfaz de navegador notifica un evento de clic de usuario a la unidad de núcleo de navegador;

403, la unidad de núcleo de navegador detecta el evento de clic de usuario y notifica el evento de clic de usuario a la unidad de aplicación web como un evento de activación de inicio de sesión;

404, la unidad de aplicación web determina una dirección de sitio web correspondiente al evento de activación de inicio de sesión y envía la dirección de sitio web a la unidad de núcleo de navegador;

405, la unidad de núcleo de navegador envía una petición de acceso al servidor de aplicación en función de la dirección de sitio web;

406, el servidor de aplicación determina que es necesario llevar a cabo una autentificación de identidad del usuario, y envía la información de indicación que necesita la autentificación de identidad a la unidad de núcleo de navegador, en la que la información de indicación de autentificación de identidad puede llevar un parámetro de restricción de autentificación de identidad;

407, la unidad de núcleo de navegador genera un evento que necesita la autentificación de identidad en función de la información de indicación que necesita la autentificación de identidad, y notifica el evento que necesita la autentificación de identidad a la unidad de aplicación web;

408, la unidad de aplicación web considera si un objeto de ventana en un DOM de navegador incluye un subobjeto de función de inicio de sesión en función del evento que necesita la autentificación de identidad, si se detecta el subobjeto de función de inicio de sesión, entonces lleva a cabo 409;

409, la invocación de una interfaz de inicio de sesión de un objeto de autentificación proporcionado en la unidad de núcleo de navegador;

410, la unidad de núcleo de navegador comprueba si la unidad de núcleo de navegador necesita seleccionar de forma automática un certificado digital para el usuario; si la selección automática no es necesaria, invoca una interfaz de gestor de certificados digitales, el usuario selecciona un certificado digital de usuario a través de una lista de certificados digitales de usuario presentados visualmente en la unidad de interfaz de navegador, y envía información de indicación de selección a la unidad de núcleo de navegador;

411, la unidad de núcleo de navegador notifica un evento de selección de certificado digital a la unidad de aplicación web;

412, la unidad de aplicación web envía un parámetro de inicio de sesión modificado a la unidad de núcleo de navegador en función del evento de selección de certificado digital;

413, la unidad de núcleo de navegador devuelve una respuesta de parámetro de inicio de sesión modificado a la unidad de aplicación web;

414, la unidad de núcleo de navegador envía una petición de inicio de sesión al servidor de aplicación, en la que la petición de inicio de sesión lleva el certificado digital de usuario seleccionado;

415, el servidor de aplicación consulta un servidor de autentificación por medio del SPARQL para obtener una identidad de usuario, recibe el resultado de consulta y considera si la autentificación de identidad de usuario se realiza correctamente; si es así, entonces lleva a cabo 416; si falla, entonces envía una respuesta de fallo de autentificación de identidad a la unidad de núcleo de navegador (no se muestra en la figura);

416, el servidor de aplicación devuelve una respuesta de éxito de autentificación de identidad a la unidad de núcleo de navegador, en la que la respuesta de éxito de autentificación de identidad lleva un fichero de página web, y el fichero de página web puede ser específicamente un fichero html/css/js;

417, la unidad de núcleo de navegador transfiere un resultado de inicio de sesión a la unidad de aplicación web a través de una interfaz de llamada de respuesta;

418, la unidad de núcleo de navegador analiza sintácticamente el fichero de página web;

419, la unidad de interfaz de navegador presenta visualmente la página web analizada sintácticamente.

En los métodos de implementación anteriores, la unidad de núcleo de navegador realiza el proceso de análisis sintáctico tanto a la información de indicación que necesita la autentificación de identidad como a la respuesta enviada por el servidor de aplicación, lo que puede reducir la complejidad de procesamiento de la unidad de aplicación Web. Naturalmente, el procedimiento de procesamiento para el análisis sintáctico de la información de indicación que necesita la autentificación de identidad y la respuesta enviada por el servidor de aplicación también puede ser implementado por la unidad de aplicación web.

La Figura 5 es un diagrama de flujo de un tercer método para la autentificación de identidad según una realización de la presente invención. Como se muestra en la Figura 5, en otro método de implementación, la implementación específica de las etapas 501-503 de esta realización puede referirse respectivamente a las etapas 201-203 como se muestran en la Figura 2 y no se repetirán en la presente memoria.

Esta realización también incluye la etapa 204 de la realización como se muestra en la Figura 2, es decir, la determinación, por la unidad de núcleo de navegador, del certificado digital de usuario seleccionado en función de la información de indicación que necesita la autentificación de identidad, y puede incluir específicamente las siguientes etapas:

etapa 504, la generación, por la unidad de núcleo de navegador, de un evento que necesita la autentificación de identidad en función de la información de indicación que necesita la autentificación de identidad, y la notificación del evento que necesita la autentificación de identidad a la unidad de aplicación web;

etapa 505, la invocación, por la unidad de aplicación web, de una interfaz de selección de certificado digital de un objeto de gestión de certificados digitales de la unidad de núcleo de navegador en función de la información de indicación que necesita la autentificación de identidad; y

etapa 506, la adquisición, por la unidad de núcleo de navegador, de un certificado digital de usuario predeterminado almacenado localmente y la determinación del certificado digital de usuario predeterminado como el certificado digital de usuario seleccionado, o la adquisición, por la unidad de núcleo de navegador, de una pluralidad de certificados digitales de usuario que se van a seleccionar que están almacenados localmente, y la determinación de un certificado digital de usuario de la pluralidad de certificados digitales de usuario que se van a seleccionar como el certificado digital de usuario seleccionado en función de la información de indicación de selección recibida.

Específicamente, la información de indicación que necesita la autentificación de identidad es específicamente una respuesta HTTP. La unidad de núcleo de navegador recibe la información de indicación que necesita la autentificación de identidad, notifica un evento que necesita la autentificación de identidad a la unidad de aplicación Web en función de la información de indicación que necesita la autentificación de identidad, y puede transferir específicamente la información de indicación que necesita la autentificación de identidad a la unidad de aplicación web invocando una interfaz de petición de protocolo de transferencia de hipertexto de la unidad de aplicación web, en la que la interfaz de petición de protocolo de transferencia de hipertexto es específicamente una interfaz de

PeticiónXMLHttp en una arquitectura de programa de aplicación web AJAX. La unidad de aplicación web determina que es necesario llevar a cabo la autentificación de identidad del usuario en función de la información de indicación que necesita la autentificación de identidad, si existe un parámetro de restricción de autentificación de identidad, la unidad de aplicación Web también puede analizar sintácticamente el parámetro de restricción de autentificación de identidad de la información de indicación que necesita la autentificación de identidad.

La unidad de aplicación web: una aplicación web considera si un objeto de ventana en un DOM de navegador incluye un subobjeto de gestión de certificados digitales, en el que el subobjeto de gestión de certificados digitales es específicamente una GestiónCertificadoDigital, si se detecta la ventana. GestiónCertificadoDigital, entonces crea un objeto de gestión de certificados digitales, es decir, el objeto GestiónCertificadoDigital invoca la interfaz de selección de certificado digital proporcionada por la unidad de núcleo de navegador, si el parámetro de restricción de autentificación de identidad existe, entonces también puede introducir el parámetro de restricción de autentificación de identidad como un parámetro dentro de la unidad de núcleo de navegador a través de la interfaz de inicio de sesión, en la que la interfaz de selección de certificado digital es específicamente una interfaz selecciónCD. La unidad de aplicación web también puede detectar si se necesita llevar a cabo la autentificación de identidad del usuario en función de una lógica interna de aplicación web.

La interfaz de selecciónCD puede ser implementada específicamente a través de las siguientes funciones de interfaz:

interfaz GestiónCertificadoDigital: ObjetivoEvento {

solo lectura [CD] atributo ListaCD;

//selección de una función de certificado digital

vacío selecciónCD (ContextoAutent contexto);

//una función de llamada de respuesta

vacío atributo Función? ActivadaSelecciónCD;//selección de una función de llamada de respuesta de certificado digital

};

La unidad de núcleo de navegador recibe la invocación a la interfaz GestiónCertificadoDigital::selecciónCD, y detecta si la unidad de núcleo de navegador necesita seleccionar de forma automática un certificado digital determinado para el usuario para la autentificación de identidad en este momento, en función de una configuración de usuario o política de sistema predeterminadas.

Si es necesario llevar a cabo la selección automática, la unidad de núcleo de navegador adquiere un certificado digital de usuario predeterminado, si el parámetro de restricción de autentificación de identidad se introduce cuando se invoca la interfaz selecciónCD, entonces también puede comprobar si el certificado digital de usuario predeterminado cumple los requisitos del parámetro de restricción de autentificación de identidad. Mediante la confirmación de la utilización del certificado digital de usuario predeterminado para llevar a cabo esta autentificación de identidad, ya no es necesario llevar a cabo una interacción explícita con el usuario a través de una interfaz de gestor de certificados digitales, lo que puede acortar el tiempo de procesamiento para el proceso global en gran medida y mejorar la eficiencia de procesamiento.

Si no es necesario llevar a cabo una selección automática, la unidad de núcleo de navegador adquiere la pluralidad de certificados digitales de usuario que se van a seleccionar para formar una lista de certificados digitales de usuario. Si el parámetro de restricción de autentificación de identidad se transfiere, también se puede llevar a cabo una comprobación y una filtración para todos los certificados digitales de usuario gestionados en función del parámetro de restricción de autentificación de identidad, y se obtiene una lista de certificados digitales de usuario disponibles. Y la interfaz de gestor de certificados digitales emerge, la cual enumera todos los certificados digitales de usuario disponibles, y provoca que el usuario seleccione un certificado digital de usuario determinado para la autentificación de identidad de este acceso de sitio web de los certificados digitales de usuario disponibles. La información de indicación de selección es concretamente información de indicación para la selección de una introducción de certificado digital de usuario determinado por el usuario. Este método de procesamiento puede facilitar que el usuario realice inicios de sesión en diferentes aplicaciones web utilizando diferentes identidades de usuario.

Durante el proceso de implementación específico, la interfaz de gestor de certificados digitales anterior puede ser una interfaz de operación del gestor de certificados digitales implementada en la unidad de núcleo de navegador, si la unidad de núcleo de navegador implementa el gestor de certificados digitales por sí misma, la unidad de núcleo de navegador necesita leer un certificado digital almacenado por el equipo local y presentar visualmente el certificado

digital en la interfaz de gestor de certificados digitales a través de una interfaz CAPICOM proporcionada por el sistema operativo; en este método de implementación, el navegador puede llevar a cabo la lectura del certificado digital de usuario cuando se está iniciando, y también puede activar la lectura del certificado digital de usuario cuando procesa una aplicación y una página específicas, para proporcionar una eficiencia de procesamiento mayor. El gestor de certificados digitales también puede ser un gestor de certificados digitales proporcionado por el sistema operativo.

Si la unidad de aplicación web preestablece una supervisión para un evento de selección de certificado digital de usuario, la unidad de núcleo de navegador notifica el evento de selección de certificado digital a la aplicación web, y transfiere el certificado digital de usuario seleccionado por el usuario como un parámetro para una capa de aplicación web a través de una interfaz de notificación de evento de selección de certificado digital. La unidad de aplicación web da instrucciones a la unidad de núcleo de navegador para que envíe la petición de inicio de sesión al servidor de aplicación.

Para las etapas 501-503 de la realización como se muestran en la Figura 5, se puede hacer referencia a las etapas 201-203 de la realización como se muestran en la Figura 2, y para las etapas 507-509 de la realización como se muestran en la Figura 5, se puede hacer referencia a las descripciones pertinentes de las etapas 205-207 de la realización como se muestran en la Figura 2, y no se repetirán en la presente memoria.

En la etapa 508 de esta realización, después de la recepción, por la unidad de núcleo de navegador, de la respuesta que indica el éxito de autentificación que es devuelta por el servidor de aplicación después de llevar a cabo la autentificación de identidad en función del certificado digital seleccionado, y antes de la extracción, por la unidad de núcleo de navegador, del fichero de página web de la respuesta, el método incluye además:

el envío, por la unidad de núcleo de navegador, de la respuesta a la unidad de aplicación web mediante la invocación de una interfaz de petición de protocolo de transferencia de hipertexto de la unidad de aplicación web;

el análisis sintáctico, por la unidad de aplicación Web, de un resultado de autentificación que indica el éxito de autentificación de la respuesta.

La interfaz de petición de protocolo de transferencia de hipertexto es específicamente una interfaz de PeticiónXMLHttp en una arquitectura de programa de aplicación web AJAX (JavaScript Asíncrono y XML). La unidad de núcleo de navegador envía la respuesta enviada por el servidor de aplicación a la unidad de aplicación web mediante la invocación de la interfaz de petición de protocolo de transferencia de hipertexto, y la unidad de aplicación web analiza sintácticamente el resultado de autentificación que indica el éxito de autentificación de la respuesta.

La Figura 6 es otro diagrama de una autentificación de identidad según una realización de la presente invención. El método para la autentificación de identidad según esta realización se ilustrará en detalle a continuación con referencia a la Figura 6.

601, un usuario hace clic en un texto, un botón o una imagen que incluye un hipervínculo en una página web presentada visualmente por una unidad de interfaz de navegador;

602, la unidad de interfaz de navegador notifica un evento de clic de usuario a la unidad de núcleo de navegador;

603, la unidad de núcleo de navegador detecta el evento de clic de usuario y notifica el evento de clic de usuario a la unidad de aplicación web como un evento de activación de inicio de sesión;

604, la unidad de aplicación Web determina una dirección de sitio web correspondiente al evento de activación de inicio de sesión, y envía la dirección de sitio web a la unidad de núcleo de navegador;

605, la unidad de núcleo de navegador envía una petición de acceso al servidor de aplicación en función de la dirección de sitio web;

606, el servidor de aplicación determina que es necesario llevar a cabo una autentificación de identidad del usuario, y envía la información de indicación que necesita la autentificación de identidad a la unidad de núcleo de navegador, en la que la información de indicación de autentificación de identidad puede llevar un parámetro de restricción de autentificación de identidad;

607, la unidad de núcleo de navegador genera un evento que necesita la autentificación de identidad en función de la información de indicación que necesita la autentificación de identidad, y notifica el evento que necesita la autentificación de identidad a la unidad de aplicación web;

608, la unidad de aplicación web considera si un objeto de ventana en un DOM de navegador incluye un subobjeto de gestión de certificados digitales en función del evento que necesita la autentificación de identidad, si se detecta el subobjeto de gestión de certificados digitales, entonces lleva a cabo 609;

609, la invocación de una interfaz de selección de certificado digital proporcionada en la unidad de núcleo de navegador;

610, la unidad de núcleo de navegador comprueba si la unidad de núcleo de navegador necesita seleccionar de forma automática un certificado digital para el usuario; si la selección automática no es necesaria, invoca una interfaz de gestor de certificados digitales, el usuario selecciona un certificado digital de usuario a través de una lista de certificados digitales de usuario presentada visualmente en la unidad de interfaz de navegador, y envía información de indicación de selección a la unidad de núcleo de navegador;

611, la unidad de núcleo de navegador transfiere un resultado de selección de certificado digital de usuario a la unidad de aplicación web a través de una interfaz de llamada de respuesta;

612, la unidad de aplicación web envía una petición de inicio de sesión a la unidad de núcleo de navegador mediante la invocación de una interfaz de petición de protocolo de transferencia de hipertexto;

613, la unidad de núcleo de navegador envía una petición de inicio de sesión al servidor de aplicación, en la que la petición de inicio de sesión lleva el certificado digital de usuario seleccionado;

614, el servidor de aplicación adquiere el certificado digital de usuario del usuario de un servidor de autentificación, recibe un certificado digital de usuario enviado por el servidor de autentificación, y hace coincidir los certificados digitales de usuario; si la coincidencia se realiza correctamente, entonces lleva a cabo 615; si la coincidencia falla, entonces devuelve una respuesta de fallo de autentificación de identidad HTTP a la unidad de núcleo de navegador (no se muestra en el dibujo);

615, el servidor de aplicación devuelve una respuesta de éxito de autentificación de identidad HTTP a la unidad de núcleo de navegador, en la que la respuesta de éxito de autentificación de identidad lleva un fichero de página web, y el fichero de página web puede ser específicamente un fichero html/css/js;

616, la unidad de núcleo de navegador transfiere la respuesta de éxito de autentificación de identidad a la unidad de aplicación web a través de la interfaz de respuesta de protocolo de transferencia de hipertexto;

617, la unidad de núcleo de navegador analiza sintácticamente el fichero de página web;

618, la unidad de interfaz de navegador presenta visualmente la página web analizada sintácticamente.

La Figura 7 es un diagrama de flujo de un cuarto método para la autentificación de identidad según una realización de la presente invención. Como se muestra en la Figura 7, en otro escenario de aplicación, un usuario inicia sesión cuando utiliza la aplicación web, en la etapa 101 de la realización como se muestra en la Figura 1, antes de la generación, por la unidad de núcleo de navegador, de la petición de inicio de sesión que lleva el certificado digital de usuario seleccionado en función del certificado digital de usuario seleccionado, y el envío de la petición de inicio de sesión al servidor de aplicación; el método también puede incluir además las siguientes etapas:

etapa 701, la recepción, por la unidad de interfaz de navegador, de información de dirección de sitio web al que se va a acceder y una identificación de identidad, y el envío de la información de dirección de sitio web al que se va a acceder y la identificación de identidad a la unidad de núcleo de navegador;

En la etapa 101 de la realización como se muestra en la Figura 1, la generación, por la unidad de núcleo de navegador, de la petición de inicio de sesión que lleva el certificado digital de usuario seleccionado en función del certificado digital de usuario seleccionado, y el envío de la petición de inicio de sesión al servidor de aplicación, puede incluir específicamente lo que sigue en esta realización:

la determinación, por la unidad de núcleo de navegador, del certificado digital de usuario seleccionado en función de la identificación de identidad, la generación de la petición de inicio de sesión que lleva el certificado digital de usuario seleccionado, y el envío de la petición de inicio de sesión al servidor de aplicación, es decir, la etapa 702 de esta realización.

El usuario introduce una dirección de sitio web en una barra de direcciones presentada visualmente por la unidad de interfaz de navegador, en la que la dirección de sitio web es concretamente información de dirección de sitio web al que se va a acceder, la unidad de interfaz de navegador proporciona una lista de WebID para el usuario, el usuario selecciona una WebID de la lista de WebID, es decir, el usuario espera acceder a una página web correspondiente a la dirección de sitio web mediante la utilización de una identidad de usuario correspondiente a la WebID, en la que la WebID es concretamente la identificación de identidad. La unidad de interfaz de navegador envía la información de dirección de sitio web al que se va a acceder y la identificación de identidad a la unidad de núcleo de navegador.

La unidad de núcleo de navegador puede proporcionar una interfaz de selección de identidad al usuario a través de una interfaz CAPICOM proporcionada por un sistema operativo, para seleccionar un certificado digital guardado por

un equipo nativo. La interfaz de selección de identidad también puede ser una interfaz de gestor de certificados digitales correspondiente al gestor de certificados digitales proporcionado por el sistema operativo.

La unidad de núcleo de navegador también puede seleccionar de forma automática una identidad de usuario determinada para el usuario para la autentificación de identidad en este momento en función de una configuración de usuario o una política de sistema, ya no es necesario llevar a cabo una interacción explícita con el usuario a través de una lista de WebID disponible o la interfaz de gestor de certificados digitales, lo que puede acortar el tiempo de procesamiento para el proceso global en gran medida y mejorar la eficiencia de procesamiento.

Para las etapas 703 y 704 de esta realización, se puede hacer referencia a las descripciones pertinentes de las etapas 102 y 103 de la realización como se muestran en la Figura 1, y no se repetirán en la presente memoria.

La Figura 8 es un diagrama de señalización de aún otra autentificación de identidad según una realización de la presente invención. El método para la autentificación de identidad según esta realización se ilustrará en detalle a continuación con referencia a la Figura 8.

801, la unidad de interfaz de navegador envía una dirección de sitio web y una introducción de WebID por el usuario a la unidad de núcleo de navegador;

802, la unidad de núcleo de navegador determina un certificado digital de usuario en función de la WebID, envía una petición de inicio de sesión que lleva el certificado digital de usuario al servidor de aplicación, específicamente, el núcleo de navegador puede utilizar una clave privada de usuario para cifrar la dirección de sitio web y un sello de tiempo, y la dirección de sitio web y el sello de tiempo se llevan como un parámetro en la petición de inicio de sesión;

803, el servidor de aplicación adquiere el certificado digital de usuario del usuario de un servidor de autentificación, recibe un certificado digital de usuario enviado por el servidor de autentificación, y hace coincidir los certificados digitales de usuario; si la coincidencia se realiza correctamente, entonces lleva a cabo 804; si la coincidencia falla, entonces devuelve una respuesta de fallo de autentificación de identidad a la unidad de núcleo de navegador (no se muestra en el dibujo), específicamente, después de recibir la petición de inicio de sesión, el servidor de aplicación utiliza una clave pública de usuario para el descifrado; si la dirección de sitio web obtenida mediante descifrado coincide con la dirección de sitio web al que el usuario está accediendo, entonces se puede determinar que la petición de inicio de sesión es emitida por un usuario de proxy de navegador efectivamente, de lo contrario la petición de inicio de sesión puede ser falsificada por un tercero por medio de una interceptación de mensaje;

804, el servidor de aplicación devuelve una respuesta de éxito de autentificación de identidad a la unidad de núcleo de navegador, en la que la respuesta de éxito de autentificación de identidad lleva un fichero de página web, y el fichero de página web es específicamente un fichero html/css/js;

805, la unidad de núcleo de navegador analiza sintácticamente el fichero de página web;

806, la unidad de interfaz de navegador presenta visualmente la página web analizada sintácticamente.

Durante el proceso de utilización de la aplicación web por el usuario, se puede detectar el estado de usuario, para evitar llevar a cabo de forma repetida una autentificación de identidad a un usuario que ha iniciado sesión.

La Figura 9 es un diagrama de flujo de un quinto método para la autentificación de identidad según una realización de la presente invención. Como se muestra en la Figura 9, esta realización difiere de la realización como se muestra en la Figura 1 en que, antes de la etapa 101 de la realización como se muestra en la Figura 1, la generación, por la unidad de núcleo de navegador, de la petición de inicio de sesión que lleva el certificado digital de usuario seleccionado en función del certificado digital de usuario seleccionado; el método según esta realización también puede incluir las siguientes etapas:

etapa 901, la detección, por la unidad de núcleo de navegador, de un evento de activación de inicio de sesión, y el envío del evento de activación de inicio de sesión a una unidad de aplicación web;

etapa 902, la determinación, por la unidad de aplicación web, de una dirección de sitio web correspondiente a una operación de activación de inicio de sesión en función del evento de activación de inicio de sesión; si se considera que el acceso al sitio web necesita la autentificación de identidad, entonces la adquisición del estado de usuario, si el estado de usuario es un estado de cierre de sesión, entonces la invocación de una interfaz de inicio de sesión de un objeto de autentificación de la unidad de núcleo de navegador;

etapa 903, la adquisición, por la unidad de núcleo de navegador, de un certificado digital de usuario predeterminado, y la determinación del certificado digital de usuario predeterminado como el certificado digital de usuario seleccionado, o la adquisición, por la unidad de núcleo de navegador, de una pluralidad de certificados digitales de usuario que se van a seleccionar, y la determinación de un certificado digital de usuario de la pluralidad de

certificados digitales de usuario que se van a seleccionar como el certificado digital de usuario seleccionado en función de la información de indicación de selección recibida.

Se puede considerar por la unidad de aplicación web si se necesita llevar a cabo la autentificación de identidad del usuario. La unidad de aplicación web determina la dirección de sitio web correspondiente a la operación de activación de inicio de sesión en función del evento de activación de inicio de sesión, en el que, para el evento de activación de inicio de sesión, se puede hacer referencia específicamente a las descripciones pertinentes del evento de activación de inicio de sesión en las realizaciones anteriores, y no se repetirán en la presente memoria. La unidad de aplicación web determina la seguridad, importancia y privacidad de los recursos de red a los que accede el usuario en función de la dirección de sitio web. Si se considera que el acceso a la dirección de sitio web necesita la autentificación de identidad, y entonces el estado de usuario se adquiere además, en el que el estado de usuario puede ser específicamente el estado de inicio de sesión o el estado de cierre de sesión. Si el estado de usuario es un estado de cierre de sesión, entonces la unidad de aplicación web invoca la interfaz de inicio de sesión del objeto de autentificación de la unidad de núcleo de navegador; para el proceso de invocación de la interfaz de inicio de sesión y el proceso de determinación del certificado digital de usuario seleccionado por la unidad de núcleo de navegador, se puede hacer referencia a las descripciones pertinentes de las realizaciones anteriores, y no se repetirán en la presente memoria.

Para las descripciones pertinentes de las etapas 904-906 de esta realización, se puede hacer referencia a las etapas 101-103 de la realización como se muestran en la Figura 1, y no se repetirán en la presente memoria.

Si, en la etapa 902, el estado de usuario adquirid es el estado de inicio de sesión, entonces en la etapa 905, antes de la extracción, por la unidad de núcleo de navegador, del fichero de página web de la respuesta, el método incluye además:

el envío, por la unidad de aplicación web, de la dirección de sitio web a la unidad de núcleo de navegador;

el envío, por la unidad de núcleo de navegador, de una petición de acceso al servidor de aplicación en función de la dirección de sitio web, y la recepción de una respuesta devuelta por el servidor de aplicación en función de la petición de acceso.

Específicamente, si el usuario ha iniciado sesión, entonces en el proceso de acceso a la página web por el usuario con posterioridad, la autentificación de identidad puede no llevarse a cabo, la unidad de aplicación web envía la dirección de sitio web a la unidad de núcleo de navegador directamente, de modo que la unidad de núcleo de navegador envía la petición de acceso al servidor de aplicación en función de la dirección de sitio web; después de que el servidor de aplicación recibe la petición de acceso, el servidor de aplicación devuelve la respuesta que lleva el fichero de página web requerido a la unidad de núcleo de navegador.

En esta realización, la adquisición, por la unidad de aplicación web, del estado de usuario del usuario indicado por el certificado digital de usuario seleccionado, puede incluir específicamente las siguientes etapas: la adquisición, por la unidad de aplicación web, del estado de usuario del usuario indicado por el certificado digital de usuario seleccionado mediante la invocación de una interfaz de consulta de estado de inicio de sesión de usuario de la unidad de núcleo de navegador.

La aplicación web puede invocar la interfaz de consulta de estado de inicio de sesión de usuario AutentificaciónwebID:: EstadoUsuarioConsulta proporcionada por la unidad de núcleo de navegador, asignar una WebID que se va a consultar mediante un parámetro, y adquirir el estado de usuario actual de la WebID. La unidad de aplicación web puede preimplementar una interfaz de llamada de respuesta EstadoUsuarioConsultaActivada, y entonces la unidad de núcleo de navegador puede notificar la unidad de aplicación web del estado de usuario por medio de la invocación de la función de llamada de respuesta EstadoUsuarioConsultaActivada. Si el usuario ha iniciado sesión, el estado de usuario devuelto por la unidad de núcleo de navegador está en línea. Si el usuario no ha iniciado sesión, el estado de usuario devuelto por la unidad de núcleo de navegador está fuera de línea. La unidad de aplicación web también puede preestablecer una supervisión para un evento de estado de inicio de sesión actual del usuario, la unidad de núcleo de navegador notifica a la unidad de aplicación web del estado de usuario por medio de la notificación de eventos.

En esta realización, el usuario puede implementar el cierre de sesión haciendo clic en un botón de “cierre de sesión” o cerrando una página web correspondiente a la aplicación web. Específicamente, la unidad de aplicación web invoca una interfaz AutentificaciónwebID:: CierreSesión de cierre de sesión de usuario proporcionada por la unidad de núcleo de navegador, y asignar la WebID que va a cerrar su sesión a través de un parámetro. La unidad de núcleo de navegador envía una petición HTTP al servidor de aplicación para el cierre de sesión de usuario, y recibe la respuesta HTTP devuelta por el servidor de aplicación. La unidad de núcleo de navegador analiza sintácticamente el resultado del cierre de sesión de usuario de la respuesta HTTP, la unidad de aplicación web puede preestablecer una supervisión para un evento de cierre de sesión de usuario, la unidad de núcleo de navegador notifica la aplicación web del resultado del cierre de sesión de usuario por medio de la notificación de eventos, la unidad de aplicación web también puede preimplementar una interfaz de llamada de respuesta CierreSesiónActivado, la unidad

de núcleo de navegador notifica a la aplicación web del resultado del cierre de sesión de usuario por medio de la invocación de una función de llamada de respuesta CierreSesiónActivado.

La Figura 10 es un diagrama estructural esquemático de un sistema para la autentificación de identidad según una realización de la presente invención. Como se muestra en la Figura 10, el sistema para la autentificación de identidad según esta realización incluye específicamente un dispositivo para la autentificación de identidad 1001 y un servidor de aplicación 1002, en el que el dispositivo para la autentificación de identidad 1001 puede implementar específicamente cada proceso del método para la autentificación de identidad según cualquier realización de la presente invención, que no se repetirán en la presente memoria. El dispositivo para la autentificación de identidad 1001 según esta realización incluye específicamente una unidad de núcleo de navegador 10011 y una unidad de interfaz de navegador 10012. La unidad de núcleo de navegador 10011 está configurada para generar una petición de inicio de sesión que lleva un certificado digital de usuario seleccionado en función del certificado digital de usuario seleccionado, enviar la petición de inicio de sesión a un servidor de aplicación 1002, recibir una respuesta que indica el éxito de autentificación que es devuelta por el servidor de aplicación 1002 después de llevar a cabo la autentificación de identidad en función del certificado digital seleccionado, extraer un fichero de página web de la respuesta, analizar sintácticamente el fichero de página web, generar una página web y enviar la página web a una unidad de interfaz de navegador 10012. La unidad de interfaz de navegador 10012 está configurada para presentar visualmente la página web.

Según el dispositivo de autentificación de identidad 1001 proporcionado por esta realización, una unidad de núcleo de navegador 10011 genera una petición de inicio de sesión que lleva un certificado digital de usuario seleccionado en función del certificado digital de usuario seleccionado, envía la petición de inicio de sesión a un servidor de aplicación 1002; la unidad de núcleo de navegador 10011 recibe una respuesta para indicar el éxito de autentificación enviada por el servidor de aplicación 1002, extrae un fichero de página web de la respuesta, analiza sintácticamente el fichero de página web, genera una página web y envía la página web a una unidad de interfaz de navegador 10012; la unidad de interfaz de navegador 10012 presenta visualmente la página web. La autentificación de identidad se lleva a cabo mediante el certificado de usuario digital de usuario; un usuario no necesita recordar un nombre de usuario y una contraseña, evitando de esta manera la interceptación de la contraseña durante un proceso de transmisión y mejorando la practicidad y la seguridad de la autentificación de identidad.

La Figura 11 es un diagrama estructural esquemático de otro sistema para la autentificación de identidad según una realización de la presente invención. Como se muestra en la Figura 11, el sistema de autentificación de identidad según esta realización incluye específicamente un dispositivo para la autentificación de identidad 111 y un servidor de aplicación 112, en el que el dispositivo para la autentificación de identidad 111 según esta realización incluye específicamente una unidad de núcleo de navegador 1111 y una unidad de interfaz de navegador 1112. En un escenario de aplicación, cuando un usuario utiliza la aplicación web a través de un navegador, si los recursos de red a los que se acceden no necesitan una autentificación de identidad, el usuario no necesita iniciar sesión. Si los recursos de red a los que accede el usuario necesitan una autentificación de identidad, entonces es necesario proporcionar un certificado digital de usuario por parte del usuario, para llevar a cabo la autentificación de identidad. Cuando el usuario hace clic en un texto, un botón o una imagen que incluye un hipervínculo en la página web presentada visualmente por la unidad de interfaz de navegador 1112, se generará un evento de clic de usuario. En esta realización, la diferencia entre esta realización y la realización como se muestra en la Figura 10 es que el dispositivo para la autentificación de identidad 111 según esta realización incluye además: una unidad de aplicación web 1113. La unidad de interfaz de navegador 1112 está configurada además para detectar un evento de activación de inicio de sesión, enviar el evento de activación de inicio de sesión a la unidad de aplicación web 1113, y enviar una petición de acceso al servidor de aplicación 112 en función de la dirección de sitio web enviada por la unidad de aplicación web 1113, recibir información que requiere la autentificación de identidad devuelta por el servidor de aplicación 112 en función de la petición de acceso, y determinar el certificado digital de usuario seleccionado en función de la información de indicación que necesita la autentificación de identidad. La unidad de aplicación web 1113 está configurada para determinar una dirección de sitio web correspondiente a una operación de activación de inicio de sesión en función del evento de activación de inicio de sesión, y enviar la dirección de sitio web a la unidad de núcleo de navegador 1111.

En esta realización, la unidad de núcleo de navegador 1111 está configurada además para generar un evento que necesita la autentificación de identidad en función de la información de indicación que necesita la autentificación de identidad, notificar el evento que necesita la autentificación de identidad a la unidad de aplicación web 1113, adquirir un certificado digital de usuario predeterminado que se almacena localmente, y determinar el certificado digital de usuario predeterminado como el certificado digital de usuario seleccionado; o la unidad de núcleo de navegador 1111 está configurada además para adquirir una pluralidad de certificados digitales de usuario que se van a seleccionar que se almacenan localmente, y determinar un certificado digital de usuario de la pluralidad de certificados digitales de usuario que se van a seleccionar como el certificado digital de usuario seleccionado en función de la información de indicación de selección recibida. La unidad de aplicación web 1113 está configurada además para recibir el evento que necesita la autentificación de identidad, e invocar una interfaz de inicio de sesión de un objeto de autentificación de la unidad de núcleo de navegador 1111.

En esta realización, la unidad de núcleo de navegador 1111 está configurada además para analizar sintácticamente un resultado de autentificación que indica un éxito de autentificación de la respuesta y enviar el resultado de autentificación a la unidad de aplicación web 1113 a través de un evento de resultado de autentificación o una función de llamada de respuesta.

En los métodos de implementación anteriores, la unidad de núcleo de navegador 1111 lleva a cabo un proceso de análisis sintáctico tanto para la información de indicación que necesita la autentificación de identidad como para la respuesta enviada por el servidor de aplicación 112, que puede reducir la complejidad de procesamiento de la unidad de aplicación web 1113. Desde luego, el procedimiento de procesamiento para el análisis sintáctico de la información de indicación que necesita la autentificación de identidad y la respuesta enviada por el servidor de aplicación 112 también pueden ser implementados por la unidad de aplicación web 1113. Entonces, en otro método de implementación:

La unidad de núcleo de navegador 1111 está configurada además para generar un evento que necesita la autentificación de identidad en función de la información de indicación que necesita la autentificación de identidad, notificar el evento que necesita la autentificación de identidad a la unidad de aplicación web 1113, adquirir un certificado digital de usuario predeterminado que se almacena localmente, y determinar el certificado digital de usuario predeterminado como el certificado digital de usuario seleccionado; o la unidad de núcleo de navegador 1111 está configurada además para adquirir una pluralidad de certificados digitales de usuario que se van a seleccionar que se almacenan localmente, y determinar un certificado digital de usuario de la pluralidad de certificados digitales de usuario que se van a seleccionar como el certificado digital de usuario seleccionado en función de la información de indicación de selección recibida. La unidad de aplicación web 1113 está configurada además para invocar una interfaz de selección de certificado digital de un objeto de gestión de certificado digital de la unidad de núcleo de navegador 1111 en función de la información de indicación que necesita la autentificación de identidad.

En esta realización, la unidad de núcleo de navegador 1111 está configurada además para enviar la respuesta a la unidad de aplicación web 1113 invocando una interfaz de petición de protocolo de transferencia de hipertexto de la unidad de aplicación web 1113. La unidad de aplicación web 1113 está configurada además para analizar sintácticamente un resultado de autentificación que indica un éxito de autentificación de la respuesta.

En otro escenario de aplicación, un usuario inicia sesión cuando utiliza la aplicación web, el usuario introduce una dirección de sitio web en una barra de direcciones presentada visualmente por la unidad de interfaz de navegador 1112, en la que la dirección de sitio web es concretamente información de dirección de sitio web al que se va a acceder, la unidad de interfaz de navegador 1112 proporciona una lista de WebID para el usuario, de modo que el usuario lleve a cabo una selección de WebID. En esta realización, la unidad de interfaz de navegador 1112 está configurada además para recibir la información de dirección de sitio web al que se va a acceder y una identificación de identidad, y enviar la información de dirección de sitio web al que se va a acceder y la identificación de identidad a la unidad de núcleo de navegador 1111. La unidad de núcleo de navegador 1111 está configurada además para determinar el certificado digital de usuario seleccionado en función de la identificación de identidad, generar la petición de inicio de sesión que lleva el certificado digital de usuario seleccionado, y enviar la petición de inicio de sesión al servidor de aplicación 112.

Durante el proceso de utilización de la aplicación web por el usuario, se puede detectar el estado de usuario, para evitar llevar a cabo repetidamente una autentificación de identidad. En esta realización, la unidad de núcleo de navegador 1111 está configurada además para detectar un evento de activación de inicio de sesión, enviar el evento de activación de inicio de sesión a una unidad de aplicación web 1113, adquirir un certificado digital de usuario predeterminado que se almacena localmente, y determinar el certificado digital de usuario predeterminado como el certificado digital de usuario seleccionado, o la unidad de núcleo de navegador 1111 está configurada además para adquirir una pluralidad de certificados digitales de usuario que se van a seleccionar que se almacenan localmente, y determinar un certificado digital de usuario de la pluralidad de certificados digitales de usuario que se van a seleccionar como el certificado digital de usuario seleccionado en función de la información de indicación de selección recibida. La unidad de aplicación web 1113 está configurada además para determinar una dirección de sitio web correspondiente a una operación de activación de inicio de sesión en función del evento de activación de inicio de sesión, si se considera que el acceso al sitio web necesita la autentificación de identidad, entonces adquirir un estado de usuario de un usuario indicado por el certificado digital de usuario seleccionado, si el estado de usuario es un estado de cierre de sesión, entonces invocar una interfaz de inicio de sesión de un objeto de autentificación de la unidad de núcleo de navegador 1111.

En esta realización, si el estado de usuario es un estado de inicio de sesión, entonces la unidad de aplicación web 1113 está configurada además para enviar la dirección de sitio web a la unidad de núcleo de navegador 1111. La unidad de núcleo de navegador 1111 está configurada además para enviar una petición de acceso al servidor de aplicación 112 en función de la dirección de sitio web, y recibir una respuesta devuelta por el servidor de aplicación 112 en función de la petición de acceso.

En esta realización, la unidad de aplicación web 1113 está configurada además para adquirir el estado de usuario del usuario indicado por el certificado digital de usuario seleccionado invocando una interfaz de consulta de estado de inicio de sesión de usuario de la unidad de núcleo de navegador 1111.

El dispositivo para la autentificación de identidad según esta realización puede ser específicamente un dispositivo tal como un ordenador personal, un portátil, un ordenador de tableta, un smartphone y similares, que esté provisto de un procesador y una memoria, el dispositivo para la autentificación de identidad está provisto de un navegador y un programa de aplicación. Las instrucciones relacionadas tanto del navegador como del programa de aplicación se almacenan en la memoria; el procesador invoca las instrucciones relacionadas en la memoria y lleva a cabo las instrucciones relacionadas, para generar la interfaz de presentación visual que se presenta visualmente mediante una pantalla del dispositivo para la autentificación de identidad, y conseguir las funciones de la unidad de núcleo de navegador, la unidad de presentación visual de navegador, y la unidad de aplicación web respectivamente. Las personas expertas en la técnica pueden entender que la totalidad o una parte de las etapas de los métodos según las realizaciones de la presente invención pueden ser implementadas por un hardware pertinente que da instrucciones de programas, en el que el programa puede almacenarse en un medio de almacenamiento legible por ordenador. Cuando el programa se ejecuta, se llevan a cabo las etapas de los métodos según las realizaciones anteriores; el medio de almacenamiento descrito anteriormente incluye: los medios de una ROM, una RAM, un disco o un CD, y similares, que pueden almacenar un código de programa.

REIVINDICACIONES

1. Un método para la autentificación de identidad, que comprende:

la detección (201, 501), por una unidad de núcleo de navegador, de un evento de activación de inicio de sesión, y el envío del evento de activación de inicio de sesión a una unidad de aplicación web;

la determinación (202, 502), por la unidad de aplicación web, de una dirección de sitio web correspondiente a una operación de activación de inicio de sesión en función del evento de activación de inicio de sesión, y el envío de la dirección de sitio web a la unidad de núcleo de navegador;

el envío (203, 503), por la unidad de núcleo de navegador, de una petición de acceso a un servidor de aplicación en función de la dirección de sitio web enviada por la unidad de aplicación; y

la recepción (204), por la unidad de núcleo de navegador, de la información de indicación que necesita la autentificación de identidad devuelta por el servidor de aplicación en función de la petición de acceso, en la que la información de indicación que necesita la autentificación de identidad lleva un parámetro de definición de autentificación de identidad, y la determinación de un certificado digital de usuario seleccionado que coincide con el parámetro de restricción de autentificación de identidad mediante la realización de una filtración de los certificados digitales de usuario en función del parámetro de definición de autentificación de identidad, en el que el parámetro de restricción de autentificación de identidad incluye uno cualquiera o más de una expedición de certificado, un tipo de certificado, un algoritmo de firma y un algoritmo de clave pública;

la generación (101, 205, 507), por la unidad de núcleo de navegador, de una petición de inicio de sesión que lleva el certificado digital de usuario seleccionado en función del certificado digital de usuario seleccionado, y el envío de la petición de inicio de sesión al servidor de aplicación;

la recepción (102, 206, 508), por la unidad de núcleo de navegador, de una respuesta que indica el éxito de autentificación que es devuelta por el servidor de aplicación después de llevar a cabo la autentificación de identidad en función del certificado digital seleccionado, la extracción de un fichero de página web de la respuesta, el análisis sintáctico del fichero de página web, la generación de una página web y el envío de la página web a una unidad de interfaz de navegador; y

la presentación visual (103, 207, 509), por la unidad de interfaz de navegador, de la página web.

2. El método para la autentificación de identidad según la reivindicación 1, en el que, la recepción, por la unidad de núcleo de navegador, de la información que necesita la autentificación de identidad devuelta por el servidor de aplicación en función de la petición de acceso, y la determinación del certificado digital de usuario seleccionado que coincide con el parámetro de restricción de autentificación de identidad mediante la realización de una filtración de los certificados digitales de usuario en función del parámetro de definición de autentificación de identidad, comprenden:

la generación, por la unidad de núcleo de navegador, de un evento que necesita la autentificación de identidad en función de la información de indicación que necesita la autentificación de identidad, y la notificación del evento que necesita la autentificación de identidad a la unidad de aplicación web;

la recepción, por la unidad de aplicación web, del evento que necesita la autentificación de identidad, y la invocación de una interfaz de inicio de sesión de un objeto de autentificación de la unidad de núcleo de navegador; y

la adquisición, por la unidad de núcleo de navegador, de un certificado digital de usuario predeterminado que se almacena localmente, la comprobación de si el certificado digital de usuario predeterminado cumple el requisito del parámetro de restricción de autentificación de identidad y, si es así, la determinación del certificado digital de usuario predeterminado como el certificado digital de usuario seleccionado, o la adquisición, por la unidad de núcleo de navegador, de una pluralidad de certificados digitales de usuario que se van a seleccionar que se almacenan localmente mediante la realización de una comprobación y una filtración de todos los certificados digitales de usuario gestionados en función del parámetro de restricción de autentificación de identidad, y la determinación de un certificado digital de usuario de la pluralidad de certificados digitales de usuario que se van a seleccionar como el certificado digital de usuario seleccionado en función de la información de indicación de selección recibida.

3. El método para la autentificación de identidad según la reivindicación 1, en el que, la recepción, por la unidad de núcleo de navegador, de la información que necesita la autentificación de identidad devuelta por el servidor de aplicación en función de la petición de acceso, y la determinación del certificado digital de usuario seleccionado en función de la información de indicación que necesita la autentificación de identidad que requiere la autentificación de identidad, comprenden:

la generación, por la unidad de núcleo de navegador, de un evento que necesita la autentificación de identidad en función de la información de indicación que necesita la autentificación de identidad, y la notificación del evento que necesita la autentificación de identidad a la unidad de aplicación web;

la llamada, por la unidad de aplicación web, de una interfaz de selección de certificado digital de un objeto de gestión de certificado digital de la unidad de núcleo de navegador en función de la información de indicación que necesita la autentificación de identidad;

la adquisición, por la unidad de núcleo de navegador, de un certificado digital de usuario predeterminado que se almacena localmente, la comprobación de si el certificado digital de usuario predeterminado cumple el requisito del parámetro de restricción de autentificación de identidad y, si es así, la determinación del certificado digital de usuario predeterminado como el certificado digital de usuario seleccionado, o la adquisición, por la unidad de núcleo de navegador, de una pluralidad de certificados digitales de usuario que se van a seleccionar que se almacenan localmente mediante la realización de una comprobación y una filtración de todos los certificados digitales de usuario gestionados en función del parámetro de restricción de autentificación de identidad, y la determinación de un certificado digital de usuario de la pluralidad de certificados digitales de usuario que se van a seleccionar como el certificado digital de usuario seleccionado en función de la información de indicación de selección recibida.

4. El método para la autentificación de identidad según la reivindicación 1 o 2, en el que, después de la recepción, por la unidad de núcleo de navegador, de la respuesta que indica el éxito de autentificación que es devuelta por el servidor de aplicación después de llevar a cabo la autentificación de identidad en función del certificado digital seleccionado, y antes de la extracción, por la unidad de núcleo de navegador, del fichero de página web de la respuesta, el método comprende además:

el análisis sintáctico, por la unidad de núcleo de navegador, de un resultado de autentificación que indica un éxito de autentificación de la respuesta, y el envío del resultado de autentificación a la unidad de aplicación web a través de un evento de resultado de autentificación o una función de llamada de respuesta.

5. El método para la autentificación de identidad según las realizaciones 1 o 3, en el que, después de la recepción, por la unidad de núcleo de navegador, de la respuesta que indica el éxito de autentificación que es devuelta por el servidor de aplicación después de llevar a cabo la autentificación de identidad en función del certificado digital seleccionado, antes de la extracción, por la unidad de núcleo de navegador, del fichero de página web de la respuesta, el método comprende además:

el envío, por la unidad de núcleo de navegador, de la respuesta a la unidad de aplicación web invocando una interfaz de petición de protocolo de transferencia de hipertexto de la unidad de aplicación web; y

el análisis sintáctico, por la unidad de aplicación web, de un resultado de autentificación que indica un éxito de autentificación de la respuesta.

6. Un dispositivo para la autentificación de identidad, que comprende: una unidad de aplicación web (1113), una unidad de núcleo de navegador (1111) y una unidad de interfaz de navegador (1112);

la unidad de aplicación web está configurada para determinar una dirección de sitio web correspondiente a una operación de activación de inicio de sesión en función de un evento de activación de inicio de sesión, y enviar la dirección de sitio web a la unidad de núcleo de navegador;

la unidad de núcleo de navegador está configurada para detectar el evento de activación de inicio de sesión, enviar el evento de activación de inicio de sesión a la unidad de aplicación web, y enviar una petición de acceso al servidor de aplicación en función de una dirección de sitio web enviada por la unidad de aplicación web, recibir la información de indicación que necesita la autentificación de identidad devuelta por el servidor de aplicación en función de la petición de acceso, en la que la información de indicación que necesita la autentificación de identidad lleva un parámetro de definición de autentificación de identidad, y determinar un certificado digital de usuario seleccionado que coincide con el parámetro de restricción de autentificación de identidad mediante la realización de una filtración de los certificados digitales de usuario en función del parámetro de definición de autentificación de identidad, en el que el parámetro de restricción de autentificación de identidad incluye uno cualquiera o más de una expedición de certificado, un tipo de certificado, un algoritmo de firma y un algoritmo de clave pública, generar una petición de inicio de sesión que lleva un certificado digital de usuario seleccionado en función del certificado digital de usuario seleccionado, enviar la petición de inicio de sesión a un servidor de aplicación, recibir una respuesta que indica el éxito de autentificación que es devuelta por el servidor de aplicación después de llevar a cabo la autentificación de identidad en función del certificado digital seleccionado, extraer un fichero de página web de la respuesta, analizar sintácticamente el fichero de página web, generar una página web y enviar la página web a una unidad de interfaz de navegador;

la unidad de interfaz de navegador está configurada para presentar visualmente la página web.

7. El dispositivo para la autentificación de identidad según la reivindicación 6, en el que:

la unidad de núcleo de navegador está configurada además para generar un evento que necesita la autentificación de identidad en función de la información de indicación que necesita la autentificación de identidad, notificar el evento que necesita la autentificación de identidad a la unidad de aplicación web, adquirir un certificado digital de usuario predeterminado que se almacena localmente, comprobar si el certificado digital de usuario predeterminado cumple el requisito del parámetro de restricción de autentificación de identidad y, si es así, determinar el certificado digital de usuario predeterminado como el certificado digital de usuario seleccionado; o la unidad de núcleo de navegador está configurada además para adquirir una pluralidad de certificados digitales de usuario que se van a seleccionar que se almacenan localmente mediante la realización de una comprobación y una filtración de todos los certificados digitales de usuario gestionados en función del parámetro de restricción de autentificación de identidad, y determinar un certificado digital de usuario de la pluralidad de certificados digitales de usuario que se van a seleccionar como el certificado digital de usuario seleccionado en función de la información de indicación de selección recibida;

la unidad de aplicación web está configurada además para recibir el evento que necesita la autentificación de identidad e invocar una interfaz de inicio de sesión de un objeto de autentificación de la unidad de núcleo de navegador.

8. El dispositivo para la autentificación de identidad según la reivindicación 6, en el que:

la unidad de núcleo de navegador está configurada además para generar un evento que necesita la autentificación de identidad en función de la información de indicación que necesita la autentificación de identidad, notificar el evento que necesita la autentificación de identidad a la unidad de aplicación web, adquirir un certificado digital de usuario predeterminado que se almacena localmente, comprobar si el certificado digital de usuario predeterminado cumple el requisito del parámetro de restricción de autentificación de identidad y, si es así, determinar el certificado digital de usuario predeterminado como el certificado digital de usuario seleccionado; o la unidad de núcleo de navegador está configurada además para adquirir una pluralidad de certificados digitales de usuario que se van a seleccionar que se almacenan localmente mediante la realización de una comprobación y una filtración de todos los certificados digitales de usuario gestionados en función del parámetro de restricción de autentificación de identidad, y determinar un certificado digital de usuario de la pluralidad de certificados digitales de usuario que se van a seleccionar como el certificado digital de usuario seleccionado en función de la información de indicación de selección recibida;

la unidad de aplicación web está configurada además para invocar una interfaz de selección de certificado digital de un objeto de gestión de certificado digital de la unidad de núcleo de navegador en función de la información de indicación que necesita la autentificación de identidad.

9. El dispositivo para la autentificación de identidad según las reivindicaciones 6 o 7, en el que:

la unidad de núcleo de navegador está configurada además para analizar sintácticamente un resultado de autenticación que indica un éxito de autentificación de la respuesta, y enviar el resultado de autentificación a la unidad de aplicación web a través de un evento de resultado de autentificación o una función de llamada de respuesta.

10. El dispositivo para la autentificación de identidad según las reivindicaciones 6 u 8, en el que:

la unidad de núcleo de navegador está configurada además para enviar la respuesta a la unidad de aplicación web invocando una interfaz de petición de protocolo de transferencia de hipertexto de la unidad de aplicación web;

la unidad de aplicación web está configurada además para analizar sintácticamente un resultado de autentificación que indica un éxito de autentificación de la respuesta.

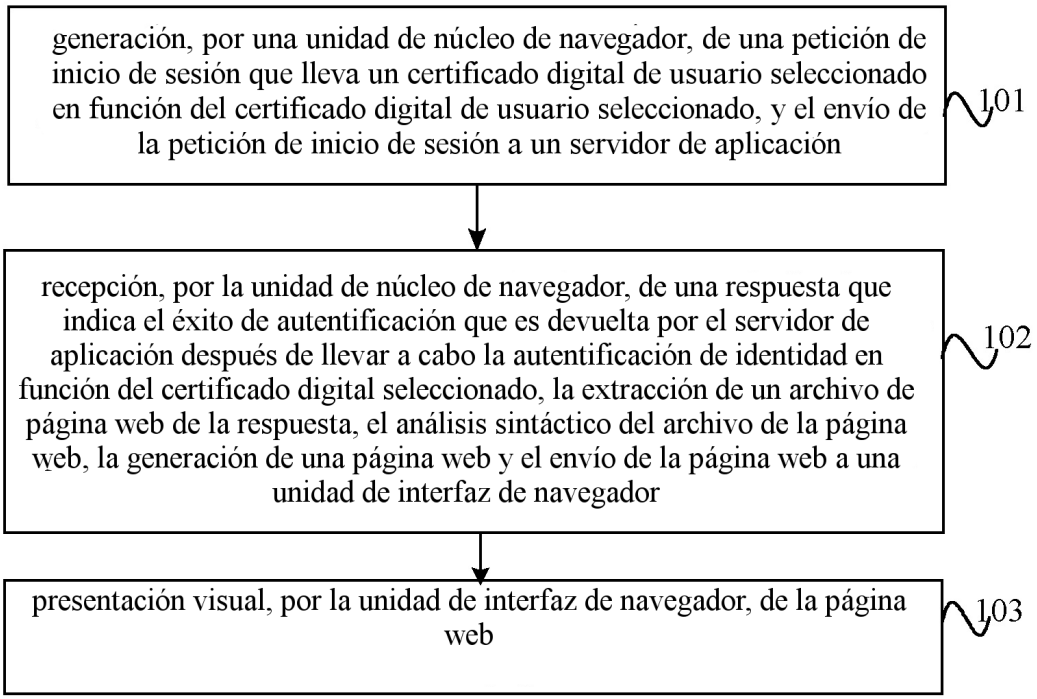
generación, por una unidad de núcleo de navegador, de una petición de inicio de sesión que lleva un certificado digital de usuario seleccionado en función del certificado digital de usuario seleccionado, y el envío de la petición de inicio de sesión a un servidor de aplicación
101
recepción, por la unidad de núcleo de navegador, de una respuesta que indica el éxito de autentificación que es devuelta por el servidor de aplicación después de llevar a cabo la autentificación de identidad en función del certificado digital seleccionado, la extracción de un archivo de página web de la respuesta, el análisis sintáctico del archivo de la página web, la generación de una página web y el envío de la página web a una unidad de interfaz de navegador
102
presentación visual, por la unidad de interfaz de navegador, de la página web
103

FIG. 1

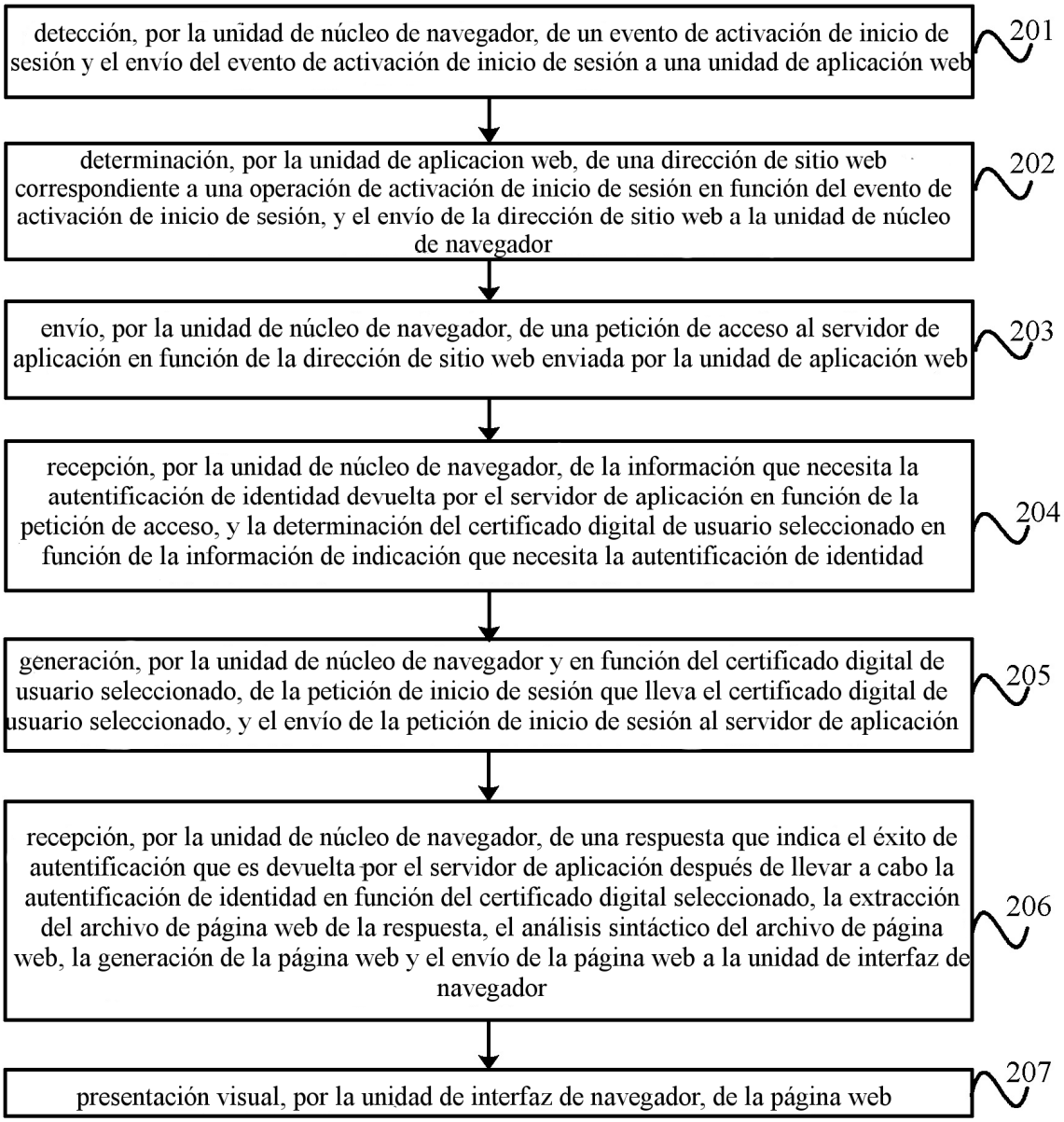
detección, por la unidad de núcleo de navegador, de un evento de activación de inicio de sesión y el envío del evento de activación de inicio de sesión a una unidad de aplicación web
201
determinación, por la unidad de aplicacion web, de una dirección de sitio web correspondiente a una operación de activación de inicio de sesión en función del evento de activación de inicio de sesión, y el envío de la dirección de sitio web a la unidad de núcleo de navegador
202
envío, por la unidad de núcleo de navegador, de una petición de acceso al servidor de aplicación en función de la dirección de sitio web enviada por la unidad de aplicación web
203
recepción, por la unidad de núcleo de navegador, de la información que necesita la autentificación de identidad devuelta por el servidor de aplicación en función de la petición de acceso, y la determinación del certificado digital de usuario seleccionado en función de la información de indicación que necesita la autentificación de identidad
204
generación, por la unidad de núcleo de navegador y en función del certificado digital de usuario seleccionado, de la petición de inicio de sesión que lleva el certificado digital de usuario seleccionado, y el envío de la petición de inicio de sesión al servidor de aplicación
205
recepción, por la unidad de núcleo de navegador, de una respuesta que indica el éxito de autentificación que es devuelta por el servidor de aplicación después de llevar a cabo la autentificación de identidad en función del certificado digital seleccionado, la extracción del archivo de página web de la respuesta, el análisis sintáctico del archivo de página web, la generación de la página web y el envío de la página web a la unidad de interfaz de navegador
206
presentación visual, por la unidad de interfaz de navegador, de la página web
207

FIG. 2

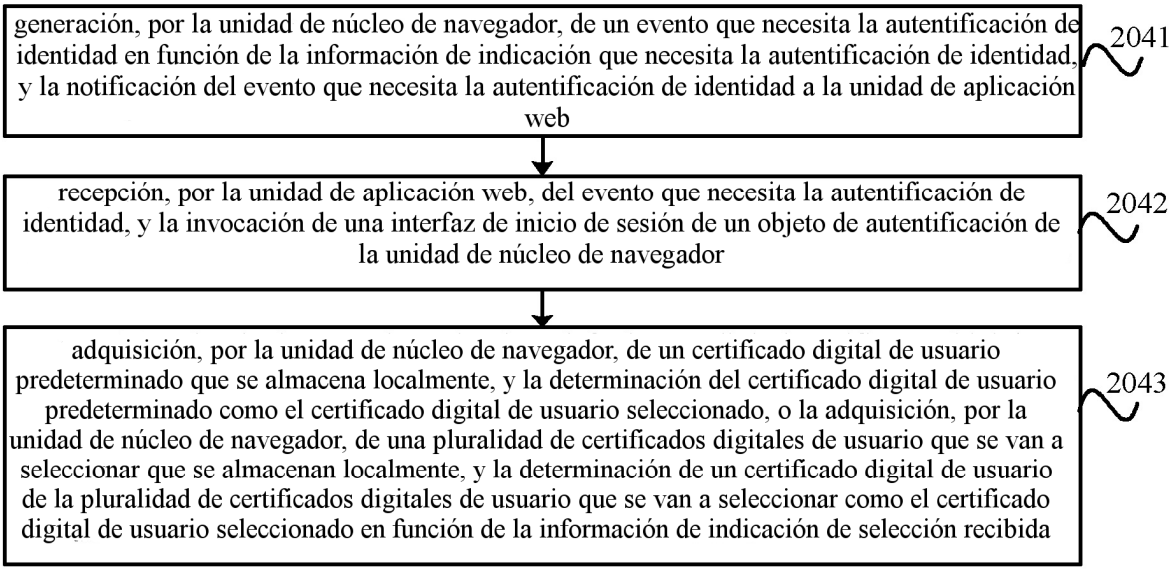
generación, por la unidad de núcleo de navegador, de un evento que necesita la autentificación de identidad en función de la información de indicación que necesita la autentificación de identidad, y la notificación del evento que necesita la autentificación de identidad a la unidad de aplicación web
2041
recepción, por la unidad de aplicación web, del evento que necesita la autentificación de identidad, y la invocación de una interfaz de inicio de sesión de un objeto de autentificación de la unidad de núcleo de navegador
2042
adquisición, por la unidad de núcleo de navegador, de un certificado digital de usuario predeterminado que se almacena localmente, y la determinación del certificado digital de usuario predeterminado como el certificado digital de usuario seleccionado, o la adquisición, por la unidad de núcleo de navegador, de una pluralidad de certificados digitales de usuario que se van a seleccionar que se almacenan localmente, y la determinación de un certificado digital de usuario de la pluralidad de certificados digitales de usuario que se van a seleccionar como el certificado digital de usuario seleccionado en función de la información de indicación de selección recibida
2043

FIG. 3

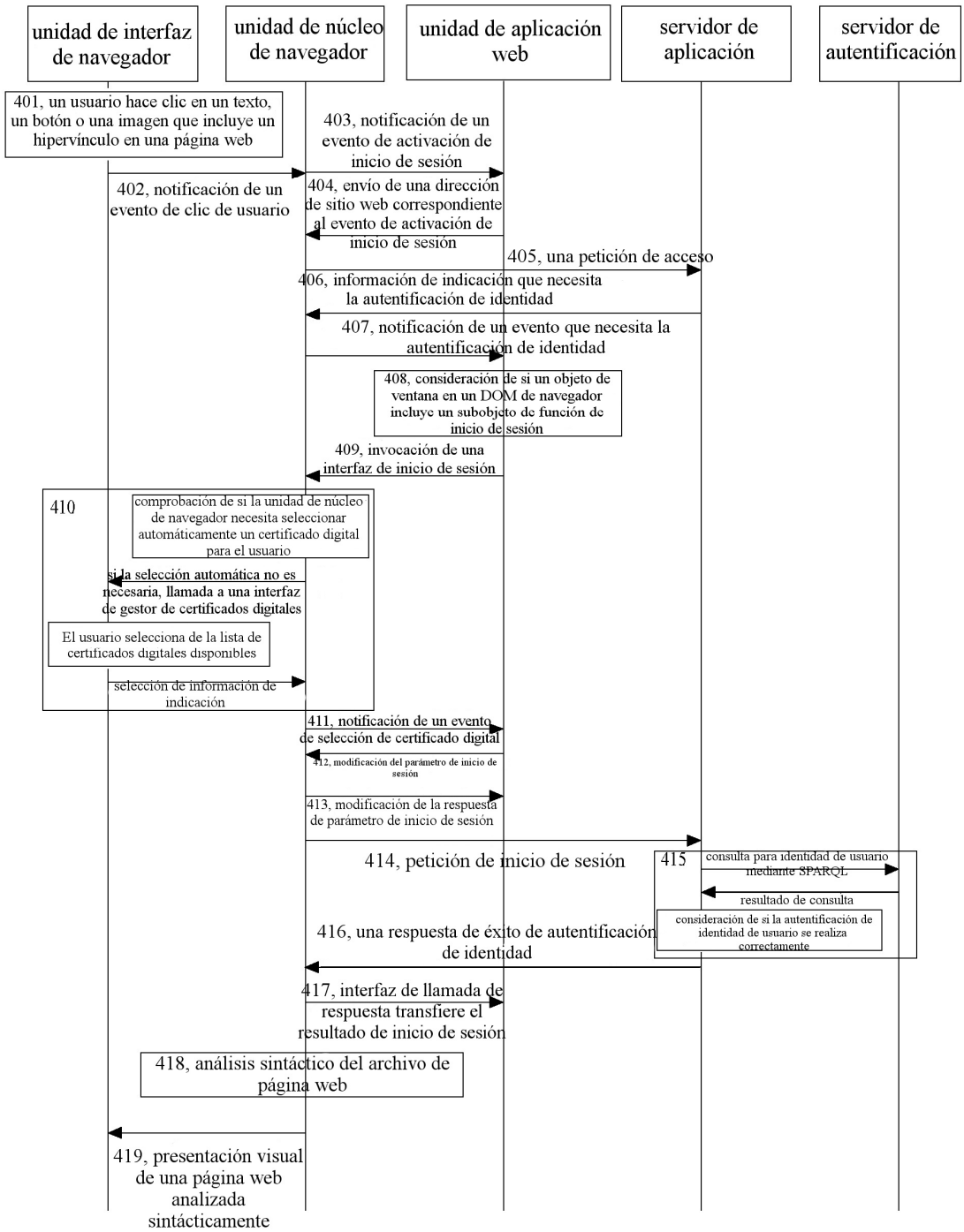
unidad de interfaz de navegador
unidad de núcleo de navegador
unidad de aplicación web
servidor de aplicación
servidor de autentificación
401, un usuario hace clic en un texto, un botón o una imagen que incluye un hipervínculo en una página web
402, notificación de un evento de clic de usuario
403, notificación de un evento de activación de inicio de sesión
404, envío de una dirección de sitio web correspondiente al evento de activación de inicio de sesión
405, una petición de acceso
406, información de indicación que necesita la autentificación de identidad
407, notificación de un evento que necesita la autentificación de identidad
408, consideración de si un objeto de ventana en un DOM de navegador incluye un subobjeto de función de inicio de sesión
409, invocación de una interfaz de inicio de sesión
410
comprobación de si la unidad de núcleo de navegador necesita seleccionar automáticamente un certificado digital para el usuario
si la selección automática no es necesaria, llamada a una interfaz de gestor de certificados digitales
El usuario selecciona de la lista de certificados digitales disponibles
selección de información de indicación
411, notificación de un evento de selección de certificado digital
412, modificación del parámetro de inicio de sesión
413, modificación de la respuesta de parámetro de inicio de sesión
414, petición de inicio de sesión
415
consulta para identidad de usuario mediante SPARQL
resultado de consulta
consideración de si la autentificación de identidad de usuario se realiza correctamente
416, una respuesta de éxito de autentificación de identidad
417, interfaz de llamada de respuesta transfiere el resultado de inicio de sesión
418, análisis sintáctico del archivo de página web
419, presentación visual de una página web analizada sintácticamente

FIG. 4

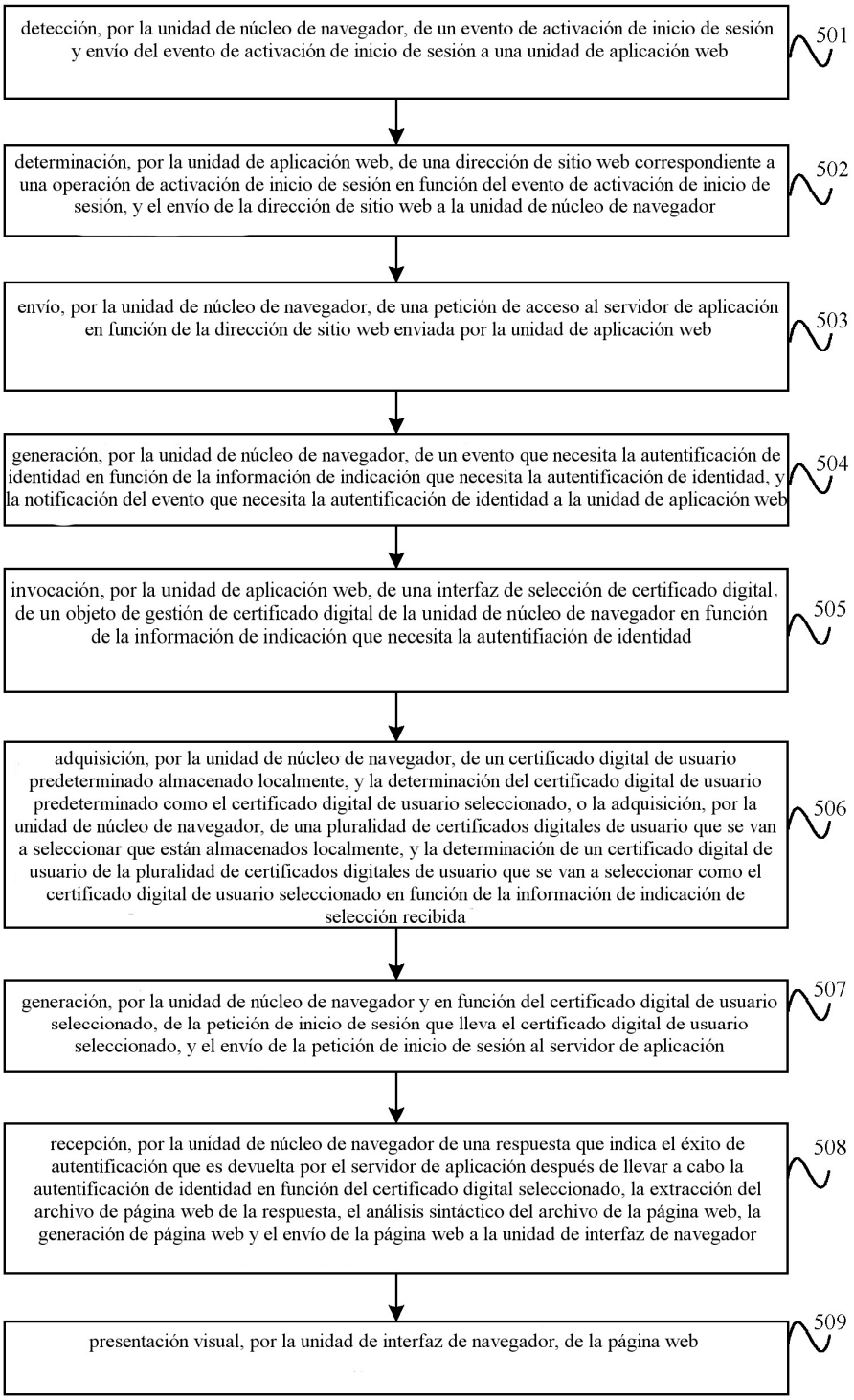
detección, por la unidad de núcleo de navegador, de un evento de activación de inicio de sesión y envío del evento de activación de inicio de sesión a una unidad de aplicación web
501
determinación, por la unidad de aplicación web, de una dirección de sitio web correspondiente a una operación de activación de inicio de sesión en función del evento de activación de inicio de sesión, y el envío de la dirección de sitio web a la unidad de núcleo de navegador
502
envío, por la unidad de núcleo de navegador, de una petición de acceso al servidor de aplicación en función de la dirección de sitio web enviada por la unidad de aplicación web
503
generación, por la unidad de núcleo de navegador, de un evento que necesita la autentificación de identidad en función de la información de indicación que necesita la autentificación de identidad, y la notificación del evento que necesita la autentificación de identidad a la unidad de aplicación web
504
invocación, por la unidad de aplicación web, de una interfaz de selección de certificado digital, de un objeto de gestión de certificado digital de la unidad de núcleo de navegador en función de la información de indicación que necesita la autentifiación de identidad
505
adquisición, por la unidad de núcleo de navegador, de un certificado digital de usuario predeterminado almacenado localmente, y la determinación del certificado digital de usuario predeterminado como el certificado digital de usuario seleccionado, o la adquisición, por la unidad de núcleo de navegador, de una pluralidad de certificados digitales de usuario que se van a seleccionar que están almacenados localmente, y la determinación de un certificado digital de usuario de la pluralidad de certificados digitales de usuario que se van a seleccionar como el certificado digital de usuario seleccionado en función de la información de indicación de selección recibida
506
generación, por la unidad de núcleo de navegador y en función del certificado digital de usuario seleccionado, de la petición de inicio de sesión que lleva el certificado digital de usuario seleccionado, y el envío de la petición de inicio de sesión al servidor de aplicación
507
recepción, por la unidad de núcleo de navegador de una respuesta que indica el éxito de autentificación que es devuelta por el servidor de aplicación después de llevar a cabo la autentificación de identidad en función del certificado digital seleccionado, la extracción del archivo de página web de la respuesta, el análisis sintáctico del archivo de la página web, la generación de página web y el envío de la página web a la unidad de interfaz de navegador
508
presentación visual, por la unidad de interfaz de navegador, de la página web
509

FIG. 5

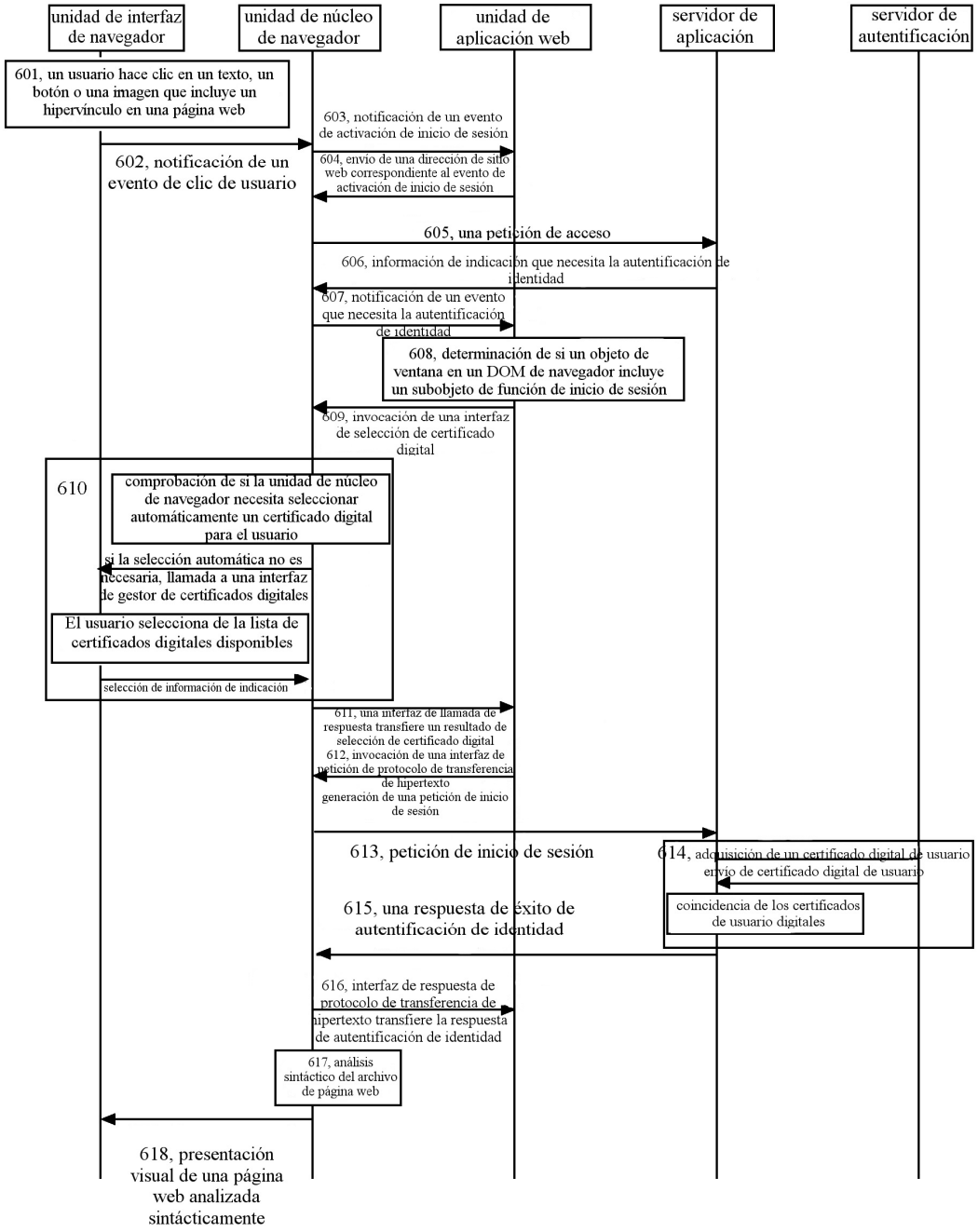
unidad de interfaz de navegador
unidad de núcleo de navegador
unidad de aplicación web
servidor de aplicación
servidor de autentificación
601, un usuario hace clic en un texto, un botón o una imagen que incluye un hipervínculo en una página web
602, notificación de un evento de clic de usuario
603, notificación de un evento de activación de inicio de sesión
604, envío de una dirección de sitio web correspondiente al evento de activación de inicio de sesión
605, una petición de acceso
606, información de indicación que necesita la autentificación de identidad
607, notificación de un evento que necesita la autentificación de identidad
608, determinación de si un objeto de ventana en un DOM de navegador incluye un subobjeto de función de inicio de sesión
609, invocación de una interfaz de selección de certificado digital
610
comprobación de si la unidad de núcleo de navegador necesita seleccionar automáticamente un certificado digital para el usuario
si la selección automática no es necesaria, llamada a una interfaz de gestor de certificados digitales
El usuario selecciona de la lista de certificados digitales disponibles
selección de información de indicación
611, una interfaz de llamada de respuesta transfiere un resultado de selección de certificado digital
612, invocación de una interfaz de petición de protocolo de transferencia de hipertexto generación de una petición de inicio de sesión
613, petición de inicio de sesión
614, adquisición de un certificado digital de usuario envío de certificado digital de usuario
coincidencia de los certificados de usuario digitales
615, una respuesta de éxito de autentificación de identidad
616, interfaz de respuesta de protocolo de transferencia de hipertexto transfiere la respuesta de autentificación de identidad
617, análisis sintáctico del archivo de página web
618, presentación visual de una página web analizada sintácticamente

FIG. 6

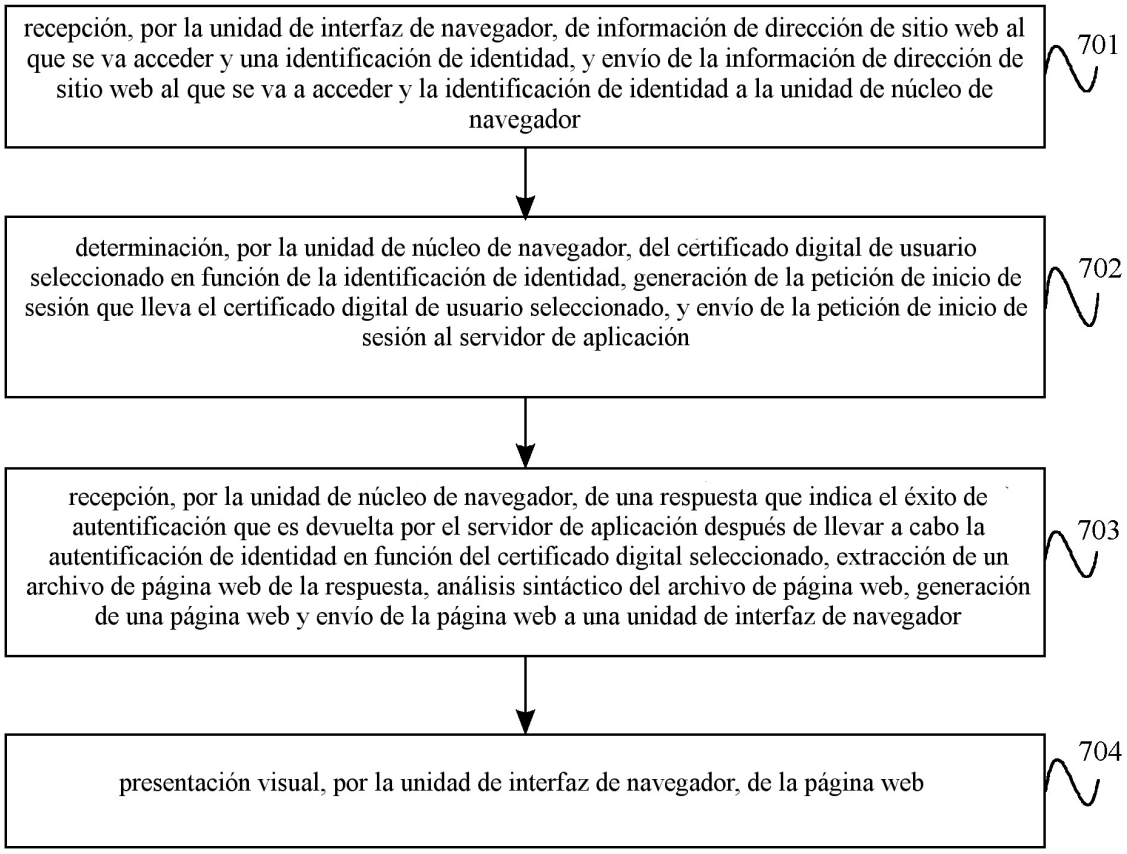
recepción, por la unidad de interfaz de navegador, de información de dirección de sitio web al que se va acceder y una identificación de identidad, y envío de la información de dirección de sitio web al que se va a acceder y la identificación de identidad a la unidad de núcleo de navegador
701
determinación, por la unidad de núcleo de navegador, del certificado digital de usuario seleccionado en función de la identificación de identidad, generación de la petición de inicio de sesión que lleva el certificado digital de usuario seleccionado, y envío de la petición de inicio de sesión al servidor de aplicación
702
recepción, por la unidad de núcleo de navegador, de una respuesta que indica el éxito de autentificación que es devuelta por el servidor de aplicación después de llevar a cabo la autentificación de identidad en función del certificado digital seleccionado, extracción de un archivo de página web de la respuesta, análisis sintáctico del archivo de página web, generación de una página web y envío de la página web a una unidad de interfaz de navegador
703
presentación visual, por la unidad de interfaz de navegador, de la página web
704

FIG. 7

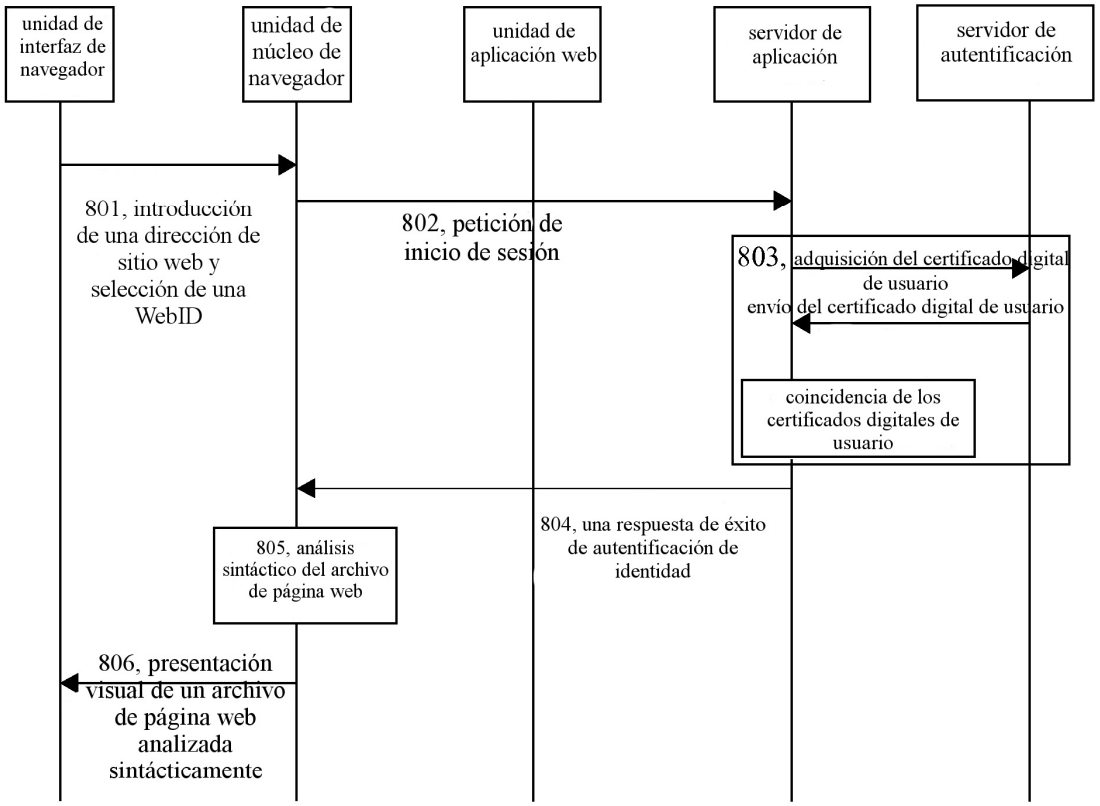
unidad de interfaz de navegador
unidad de núcleo de navegador
unidad de aplicación web
servidor de aplicación
servidor de autentificación
801, introducción de una dirección de sitio web y selección de una WebID
802, petición de inicio de sesión
803, adquisición del certificado digital de usuario
envío del certificado digital de usuario
coincidencia de los certificados digitales de usuario
804, una respuesta de éxito de autentificación de identidad
805, análisis sintáctico del archivo de página web
806, presentación visual de un archivo de página web analizada sintácticamente

FIG. 8

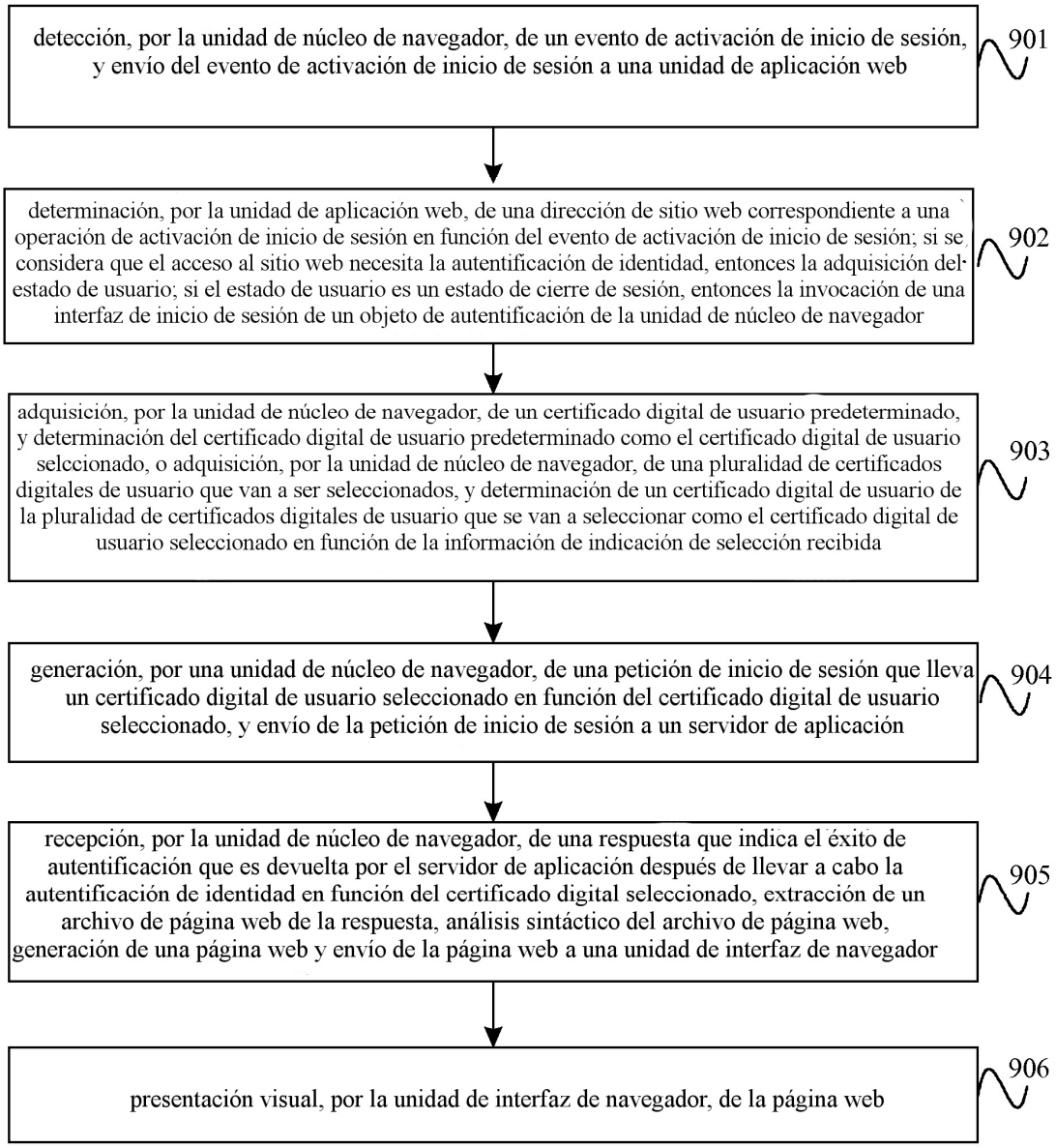
detección, por la unidad de núcleo de navegador, de un evento de activación de inicio de sesión, y envío del evento de activación de inicio de sesión a una unidad de aplicación web
901
determinación, por la unidad de aplicación web, de una dirección de sitio web correspondiente a una operación de activación de inicio de sesión en función del evento de activación de inicio de sesión; si se considera que el acceso al sitio web necesita la autentificación de identidad, entonces la adquisición del estado de usuario; si el estado de usuario es un estado de cierre de sesión, entonces la invocación de una interfaz de inicio de sesión de un objeto de autentificación de la unidad de núcleo de navegador
902
adquisición, por la unidad de núcleo de navegador, de un certificado digital de usuario predeterminado, y determinación del certificado digital de usuario predeterminado como el certificado digital de usuario selccionado, o adquisición, por la unidad de núcleo de navegador, de una pluralidad de certificados digitales de usuario que van a ser seleccionados, y determinación de un certificado digital de usuario de la pluralidad de certificados digitales de usuario que se van a seleccionar como el certificado digital de usuario seleccionado en función de la información de indicación de selección recibida
903
generación, por una unidad de núcleo de navegador, de una petición de inicio de sesión que lleva un certificado digital de usuario seleccionado en función del certificado digital de usuario seleccionado, y envío de la petición de inicio de sesión a un servidor de aplicación
904
recepción, por la unidad de núcleo de navegador, de una respuesta que indica el éxito de autentificación que es devuelta por el servidor de aplicación después de llevar a cabo la autentificación de identidad en función del certificado digital seleccionado, extracción de un archivo de página web de la respuesta, análisis sintáctico del archivo de página web, generación de una página web y envío de la página web a una unidad de interfaz de navegador
905
presentación visual, por la unidad de interfaz de navegador, de la página web
906

FIG. 9

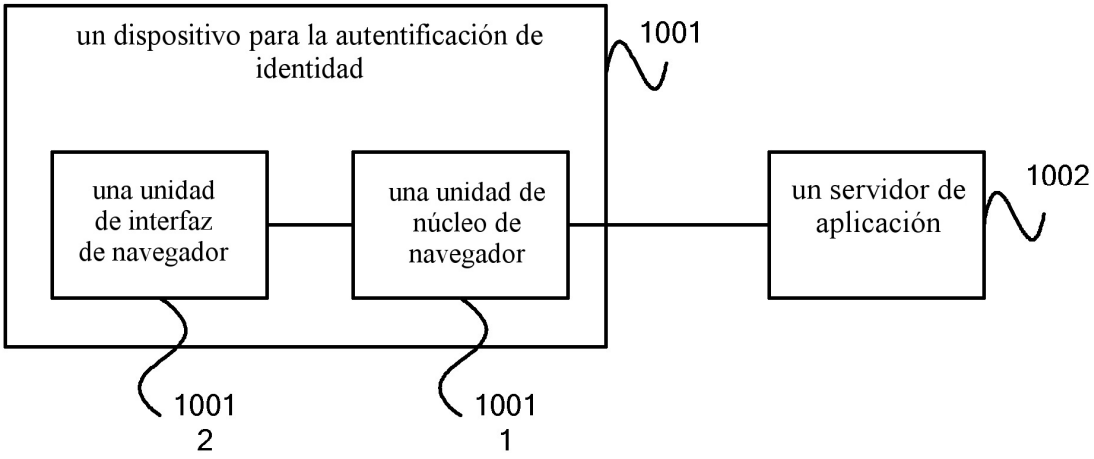
un dispositivo para la autentificación de identidad
1001
una unidad de interfaz de navegador
una unidad de núcleo de navegador
un servidor de aplicación
1002
1001 2
1001 1

FIG. 10

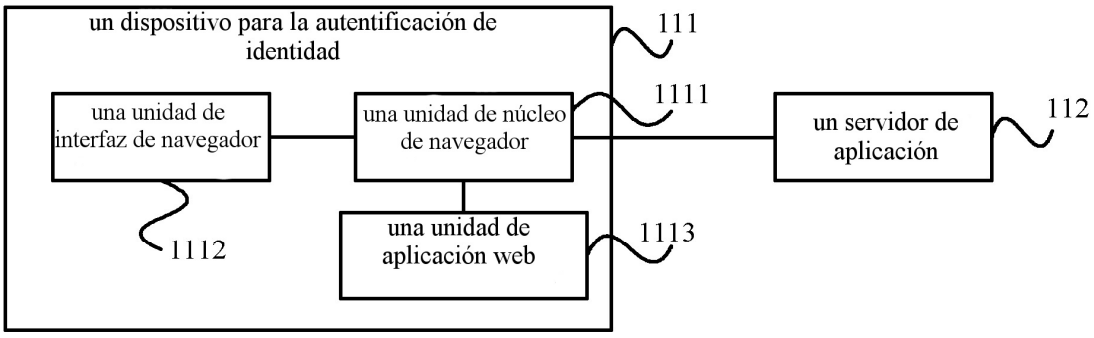
un dispositivo para la autentificación de identidad
111
una unidad de interfaz de navegador
una unidad de núcleo de navegador
1111
un servidor de aplicación
112
1112
una unidad de aplicación web
1113

FIG. 11