(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 804 471**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/57 (2013.01)
G06Q 20/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.12.2015 PCT/CN2015/096797**

(87) Fecha y número de publicación internacional: **23.06.2016 WO16095739**

(96) Fecha de presentación y número de la solicitud europea: **09.12.2015 E 15869247 (5)**

(97) Fecha y número de publicación de la concesión europea: **24.06.2020 EP 3236630**

(54) Título: **Método y dispositivo de autenticación de aparato**

(30) Prioridad:

18.12.2014 CN 201410797833

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.02.2021

(73) Titular/es:

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

(72) Inventor/es:

GUO, HONGHAI y
LI, XIAOFENG

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Método y dispositivo de autenticación de aparato

Campo técnico

La presente invención se refiere a tecnologías de seguridad de redes y, en particular, a métodos y aparatos de verificación de dispositivos.

Antecedentes

Con el desarrollo de la tecnología de redes, se está prestando más atención al tema de la seguridad de la red. Por ejemplo, en muchos servicios de sitios web, se debe identificar un dispositivo que realiza un servicio, determinando así si el dispositivo es un dispositivo seguro, para garantizar la seguridad del procesamiento del servicio. Sin embargo, en las tecnologías actuales de verificación de dispositivos, un dispositivo se identifica únicamente de acuerdo con un atributo de hardware del dispositivo, se producen fácilmente casos de peligro de seguridad, tal como la falsificación, y el método de verificación tiene baja confiabilidad.

La publicación de solicitud de patente de EE. UU. No. 2014/0351912 está dirigida a un método de identificación de terminal, y un método, sistema y aparato para registrar el código de identificación de la máquina. La solicitud de patente del Reino Unido No. 2 434 724 está dirigida a transacciones seguras utilizando tokens de autenticación basados en una "huella digital" del dispositivo derivada de sus parámetros físicos.

Resumen

En vista de esto, la presente invención proporciona métodos y aparatos de verificación de dispositivo, para mejorar la fiabilidad de la verificación del dispositivo.

Específicamente, la presente invención se implementa a través de la siguiente solución técnica:

En un primer aspecto, se proporciona un método de verificación del dispositivo de acuerdo con la reivindicación 1. En un segundo aspecto, se proporciona un aparato de verificación de dispositivo de acuerdo con la reivindicación 4. Las modalidades específicas se exponen en las reivindicaciones dependientes.

En los métodos y aparatos de verificación del dispositivo de la modalidad de la presente invención, un dispositivo objetivo transporta un certificado de dispositivo cuando solicita la verificación, el certificado de dispositivo incluye una huella digital del dispositivo generada de acuerdo con un atributo del dispositivo. El dispositivo objetivo se verifica de acuerdo con el certificado del dispositivo y la huella digital del dispositivo, y el dispositivo objetivo solo puede acceder a un servicio cuando se determina que la huella del dispositivo coincide con el atributo del dispositivo objetivo y el certificado es un certificado de dispositivo objetivo, de manera que un dispositivo de acceso ilegal se pueda identificar de manera más eficiente y la verificación del dispositivo sea más confiable.

Breve descripción de las figuras

La Figura 1 es un diagrama de escenario de aplicación de un método de verificación de dispositivo de acuerdo con una modalidad de la presente invención;
La Figura 2 es un diagrama de señalización esquemático de un método de verificación de dispositivo de acuerdo con una modalidad de la presente invención;
La Figura 3 es un diagrama de señalización esquemático de otro método de verificación de dispositivo de acuerdo con una modalidad de la presente invención;
La Figura 4 es un diagrama estructural esquemático de un aparato de verificación de dispositivo de acuerdo con una modalidad de la presente invención;
La Figura 5 es un diagrama estructural esquemático de otro aparato de verificación de dispositivo de acuerdo con una modalidad de la presente invención;
La Figura 6 es un diagrama estructural esquemático de otro aparato de verificación de dispositivo de acuerdo con una modalidad de la presente invención; y
La Figura 7 es un diagrama estructural esquemático de otro aparato de verificación de dispositivo de acuerdo con una modalidad de la presente invención.

Descripción detallada

La Figura 1 muestra esquemáticamente un escenario de aplicación de un método de verificación de dispositivo de acuerdo con una modalidad de la presente invención. Como se muestra en la Figura 1, tomando como ejemplo a un usuario que realiza un servicio de pago en un sitio web, el servicio de pago es, por ejemplo, una operación de servicio, tal como el usuario paga por un servicio utilizando su propia cuenta. El usuario generalmente usa su ordenador 11 para realizar el servicio de pago; como el servicio requiere una mayor seguridad, un servidor 12 puede registrar una correspondencia

entre la cuenta del usuario y el ordenador 11 que usualmente usa el usuario, y si la cuenta del usuario se usa en el ordenador 11, el servidor 12 puede considerar que el servicio se realiza de forma segura. Si el servidor 12 descubre que la cuenta usa un ordenador 13 cuando solicita realizar un servicio de pago, en lugar del ordenador que usualmente usa el usuario, el servidor 12 puede sospechar si la cuenta del usuario ha sido adquirida ilegalmente por un hacker, y el hacker opera ilegalmente usando el ordenador 13, de manera que el servidor 12 puede rechazar realizar del servicio.

El ejemplo anterior es un escenario de aplicación de verificación de dispositivo, es decir, un servidor de sitio web identifica un dispositivo (por ejemplo, un ordenador) para garantizar la seguridad de un servicio, para verificar si el servicio se realiza de manera segura. El método de verificación del dispositivo de acuerdo con las modalidades de la presente invención que se describe posteriormente describe cómo el servidor verifica el dispositivo, para garantizar que el resultado de la verificación sea más preciso y confiable. Definitivamente, el ejemplo de verificación del dispositivo no se limita al escenario que se muestra en la Figura 1, y otros escenarios similares también pueden adoptar el método de verificación del dispositivo de acuerdo con las modalidades de la presente invención.

La Figura 2 es un diagrama de señalización esquemático de un método de verificación de dispositivo de acuerdo con una modalidad de la presente invención; como se muestra en la Figura 2, el método muestra esquemáticamente un flujo de verificación de dispositivo realizado entre un dispositivo y un servidor, por ejemplo, un usuario está utilizando el dispositivo para realizar un servicio de pago, un lado del servidor puede indicar al dispositivo que realice la verificación para garantizar la seguridad del servicio, y el servidor puede permitir que el dispositivo reanude el servicio solo después de que la verificación sea exitosa.

El siguiente proceso describe el procesamiento realizado después de que el dispositivo recibe las instrucciones del servidor solicitando que se verifique. El dispositivo que debe verificarse puede denominarse dispositivo objetivo, y un servicio a realizar por el dispositivo se denomina servicio objetivo.

201. El dispositivo objetivo recopila la primera información de atributo de dispositivo.

Después de que el dispositivo objetivo que se va a verificar recibe una instrucción que solicita la verificación del dispositivo enviada por el servidor, el dispositivo objetivo recopilará la primera información de atributo de dispositivo (la "primera" se usa simplemente para distinguirse de otra información de atributo que aparece en la siguiente modalidad, y no tiene otros significados limitativos) correspondiente al dispositivo objetivo en sí. Específicamente, la primera información de atributo de dispositivo es un atributo inherente de hardware del dispositivo objetivo.

Por ejemplo, al tomar como ejemplo el dispositivo objetivo como un ordenador, el ordenador tiene varios hardware, tal como una tarjeta de red, una tarjeta de visualización, una CPU y un chip de memoria, y se debe recopilar información de atributos del hardware como tal. Por ejemplo, para la tarjeta de visualización, los atributos de la tarjeta de visualización pueden incluir, por ejemplo, modelo, nombre, identificación de entrega, resolución y similares. Todo esto puede denominarse información de atributos del hardware, en este caso, la tarjeta de visualización. Los atributos que se recopilan específicamente, por ejemplo, si se recopila el modelo o la identificación de entrega, no están limitados en esta modalidad. Sin embargo, existe un requisito para el atributo de hardware adquirido: el atributo es un atributo inherente del hardware, es decir, un atributo sin cambios para el hardware. Por ejemplo, aún utilizando la tarjeta de visualización como ejemplo, se puede recopilar una identificación de entrega o un modelo, estos atributos son fijos y sin cambios, mientras que la resolución, aunque sea un atributo de la tarjeta de visualización, se puede cambiar, por ejemplo, después de ajustar la configuración del ordenador, la resolución se puede aumentar o reducir, y dicha información de atributo variable no se puede recopilar como la primera información de atributo de dispositivo.

Además, generalmente puede haber varias piezas de información de atributos del primer dispositivo recopiladas en esta etapa, por ejemplo, se pueden recopilar tres piezas de información de atributos o cinco piezas de información de atributos. Debe notarse que, las múltiples piezas de información de atributos pueden ser múltiples atributos correspondientes a una pieza de hardware, y también pueden ser múltiples atributos correspondientes a múltiples piezas de hardware respectivamente.

Por ejemplo, suponiendo que se recopilan tres piezas de información de atributos, a saber, un atributo A, un atributo B y un atributo C, en donde los tres atributos corresponden a una misma pieza de hardware, tal como la tarjeta de visualización, y son un modelo, una identificación de entrega y un nombre de la tarjeta de visualización respectivamente; o los tres atributos corresponden a diferentes piezas de hardware respectivamente, por ejemplo, el atributo A es un modelo de la tarjeta de red, el atributo B es una identificación de entrega de la tarjeta de visualización, el atributo C es un modelo de la CPU y similares. Definitivamente existen otros ejemplos, que no se describen en detalle aquí.

202. El dispositivo objetivo envía una solicitud de verificación de dispositivo al servidor, la solicitud incluye: un certificado de dispositivo y la primera información de atributo de dispositivo del dispositivo objetivo, el certificado de dispositivo incluye una huella digital de dispositivo generada de acuerdo con la segunda información de atributo de dispositivo.

Después de recopilar la primera información de atributo de dispositivo, el dispositivo objetivo envía una solicitud de verificación del dispositivo al servidor, para solicitarle al servidor que realice la verificación del dispositivo en el dispositivo

objetivo. La solicitud de verificación no solo incluye la primera información de atributo de dispositivo recopilada en 201, sino que también incluye un certificado del dispositivo.

En general, suponiendo que el dispositivo objetivo es un equipo de usuario legal, el servidor emite el certificado del dispositivo al dispositivo objetivo antes de este proceso de verificación del dispositivo, el dispositivo objetivo almacena el certificado de dispositivo enviado por el servidor y solo es necesario para transporta el certificado del dispositivo en la solicitud de verificación en esta etapa. En este punto, la huella digital del dispositivo generada de acuerdo con la segunda información de atributo de dispositivo y transportada en el certificado del dispositivo es una huella digital generada por el dispositivo objetivo de acuerdo con sus atributos, por ejemplo, los atributos enumerados en 201.

Suponiendo que el dispositivo objetivo que debe verificarse es un dispositivo ilegal utilizado por un hacker, el certificado del dispositivo puede ser un certificado de dispositivo de un usuario legal, que ha sido robado por el hacker, la huella digital del dispositivo incluida en el certificado del dispositivo sigue siendo la huella digital generada por el dispositivo objetivo de acuerdo con sus atributos. El hacker no puede modificar la huella digital del dispositivo incluida en el certificado del dispositivo, ya que cualquier modificación realizada en el contenido del certificado del dispositivo invalidará el certificado.

Opcionalmente, el certificado del dispositivo puede almacenarse en un módulo de plataforma confiable TPM del dispositivo objetivo, y el hardware de la TPM puede proporcionar una garantía de seguridad más confiable para el almacenamiento del certificado.

203. El servidor determina si la primera información de atributo de dispositivo coincide con la huella digital del dispositivo en el certificado del dispositivo.

Antes de que el servidor determine si la primera información de atributo de dispositivo coincide con la huella digital del dispositivo en el certificado del dispositivo en esta etapa, el servidor determina, de acuerdo con la huella digital del dispositivo, si el certificado del dispositivo es válido. Por ejemplo, al determinar que el certificado es válido, puede verificar si la huella digital del dispositivo se ha dañado, por ejemplo, el servidor puede comparar la huella digital del dispositivo en el certificado con una huella digital almacenada en el servidor previamente para determinar si la huella digital del dispositivo está dañada; el servidor también puede usar la huella digital del dispositivo para realizar una prueba de integridad para determinar si el contenido del certificado está completo y similares.

Una vez que se determina que el certificado es válido, el servidor compara la primera información de atributo de dispositivo enviada por el dispositivo objetivo en 202 con la huella digital del dispositivo en el certificado, para determinar si las dos coinciden entre sí.

Opcionalmente, puede haber dos formas en que la primera información de atributo de dispositivo coincide con la huella digital del dispositivo en el certificado. Por ejemplo, la primera información de atributo de dispositivo coincide con la segunda información de atributo de dispositivo, por ejemplo, la primera información de atributo de dispositivo recopilada por el dispositivo objetivo incluye: un atributo A, un atributo B y un atributo C, y la segunda información de atributo de dispositivo para la generación de la huella digital del dispositivo en el certificado también incluye: el atributo A, el atributo B y el atributo C, es decir, la huella digital del dispositivo también se genera de acuerdo con los tres atributos, entonces, la primera información de atributo de dispositivo coincide con la segunda información de atributo de dispositivo; en otras palabras, la primera información de atributo de dispositivo coincide con la huella digital del dispositivo en el certificado. Para otro ejemplo, también se puede generar otra huella digital de dispositivo de acuerdo con la primera información de atributo de dispositivo recopilada por el dispositivo objetivo, y si la huella digital de otro dispositivo es la misma que la huella digital del dispositivo en el certificado del dispositivo, esto indica que la primera información de atributo de dispositivo coincide con la huella digital del dispositivo en el certificado.

Además, cuando la primera información de atributo de dispositivo coincide con la segunda información de atributo de dispositivo, la coincidencia entre la información de atributo se refiere a que, por ejemplo, los valores de atributo correspondientes en la primera información de atributo de dispositivo y la segunda información de atributo de dispositivo son iguales, o una proporción del número de valores de atributo idénticos al número total de valores de atributo alcanza un umbral de proporción preestablecido.

Por ejemplo, suponiendo que hay cuatro atributos: un atributo A, un atributo B, un atributo C y un atributo D, el servidor puede comparar si los cuatro atributos recopilados por el dispositivo objetivo son idénticos a los cuatro atributos correspondientes en el dispositivo certificado. Al tomar una tarjeta de red como ejemplo, el atributo A en el certificado del dispositivo es una identificación de entrega de la tarjeta de red, la primera información de atributo de dispositivo recopilada por el dispositivo objetivo también tiene una identificación de entrega de una tarjeta de red del dispositivo objetivo, y el servidor puede comparar si las dos identificaciones de entrega son iguales, es decir, si los atributos de un tipo correspondiente del mismo hardware son iguales; y se requiere la comparación anterior para cada atributo en el certificado.

Durante la comparación, puede haber tres casos: en un caso, los valores de los atributos (los valores de los atributos son, por ejemplo, identificación de entrega de tarjetas de red) son los mismos, por ejemplo, las identificaciones de entrega son

idénticas; en otro caso, los valores de los atributos son diferentes, por ejemplo, las identificaciones de entrega son diferentes o los modelos de tarjetas de visualización son diferentes; en otro caso, el valor del atributo recopilado es nulo, por ejemplo, un atributo en el certificado del dispositivo es un modelo de una tarjeta de red, pero en la primera información de atributo de dispositivo recopilada por el dispositivo objetivo, el modelo de la tarjeta de red es nulo, es decir, no se recopila ningún modelo de tarjeta de red, esto puede verse afectado por un entorno de recopilación u otros factores durante la recopilación y el atributo no se adquiere.

Sobre la base de los tres casos de comparación anteriores, la coincidencia entre la información de atributo se puede definir como:

Por ejemplo, los valores de atributo correspondientes en la primera información de atributo de dispositivo y la segunda información de atributo de dispositivo deben ser completamente iguales, es decir, el dispositivo objetivo debe recopilar todos los valores de atributo en el certificado y los valores de atributo deben ser los mismos; entonces el servidor puede determinar que la primera información de atributo de dispositivo coincide con la segunda información de atributo de dispositivo.

Para otro ejemplo, los valores de atributo correspondientes en la primera información de atributo de dispositivo y la segunda información de atributo de dispositivo deben ser completamente iguales, en donde puede permitirse que algunos valores de atributo correspondientes recopilados sean nulos, pero no está permitido que todos los valores de atributo recopilados sean nulos; si el dispositivo objetivo no recopila ningún valor de atributo en el certificado, y todos son nulos, el servidor determina que la primera información de atributo de dispositivo no coincide con la segunda información de atributo de dispositivo; para los cuatro atributos A, B, C y D, si solo el atributo B no es recopilado por el dispositivo objetivo y los otros valores de los atributos son iguales, entonces el atributo A puede ignorarse y se determina que la primera información de atributo de dispositivo coincide con la segunda información de atributo de dispositivo.

Para otro ejemplo, entre los valores de atributo correspondientes en la primera información de atributo de dispositivo y la segunda información de atributo de dispositivo, una proporción del número de valores de atributo idénticos al número total de valores de atributo alcanza un umbral de proporción preestablecido. Por ejemplo, en los cuatro atributos anteriores, cuando solo un atributo correspondiente es diferente durante la comparación, mientras que los otros tres son iguales, la proporción del número de valores de atributo idénticos al número total de valores de atributo es 3/4, mayor que un umbral de proporción preestablecido 1/2, luego se determina que coinciden entre sí; si los valores de tres atributos son diferentes, la proporción del número de valores de atributo idénticos al número total de valores de atributo es 1/4, menor que el umbral de proporción preestablecido 1/2, entonces se determina que no coinciden entre sí.

Cabe señalar que los ejemplos de las condiciones de coincidencia descritas anteriormente son meramente ejemplos, en lugar de exhaustivos, y en una implementación específica, la condición de coincidencia puede establecerse de manera flexible de acuerdo con el grado de rigurosidad del control de seguridad requerido por la verificación del dispositivo.

La comparación de atributos en esta etapa se ilustra en combinación con el ejemplo del escenario de aplicación que se muestra en la Figura 1, y se describe cómo el servidor determina si el dispositivo es seguro y si el dispositivo es seguro o ilegal:

En la Figura 1, suponiendo que el usuario es un usuario legal, y usa su ordenador 11 para acceder al servidor 12, luego, cuando el ordenador 11 envía una solicitud de verificación del dispositivo, un certificado del dispositivo transportado en esta es un certificado emitido por el servidor 12 al ordenador 11, en donde la segunda información de atributo de dispositivo en el certificado son atributos correspondientes al ordenador 11, por ejemplo, un atributo de tarjeta de visualización y un atributo de tarjeta de red del ordenador 11; cuando se envía la solicitud de verificación del dispositivo, los atributos de la tarjeta de visualización y de la tarjeta de red del ordenador 11 también se encuentran en la primera información de atributo recopilada por el ordenador 11, y las dos piezas de información de atributo son generalmente consistentes cuando lo determina el lado del servidor.

En consecuencia, en la Figura 1, suponiendo que el usuario es un usuario ilegal que roba un certificado de dispositivo correspondiente al ordenador 11 del usuario legal y accede al servidor 12 a través del ordenador 13, y suponiendo que cuando el ordenador 13 envía una solicitud de verificación del dispositivo, el certificado del dispositivo transportado en esta es un certificado emitido por el servidor 12 al ordenador 11, y la huella digital del dispositivo en el certificado se genera de acuerdo con los atributos del ordenador 11, mientras que la primera información de atributo de dispositivo recopilada por el ordenador 13 es información de hardware correspondiente al ordenador 13 y, por lo tanto, cuando el lado del servidor determina, se determinará que la huella digital del dispositivo y la información de los atributos del primer dispositivo no coinciden entre sí.

En esta etapa, si se determina que el certificado del dispositivo es válido de acuerdo con la huella digital del dispositivo, y el resultado de la determinación es que la huella digital del dispositivo en el certificado del dispositivo coincide con la primera información de atributo de dispositivo, esto indica que el certificado del dispositivo es el certificado de dispositivo objetivo, y se lleva a cabo 204; de lo contrario, se lleva a cabo 205.

204. El servidor permite que el dispositivo objetivo realice el servicio objetivo.

En esta etapa, el servidor puede devolver una respuesta de verificación exitosa al dispositivo objetivo, o directamente permitir que el dispositivo objetivo realice una operación de servicio posterior sin devolver una respuesta exitosa.

205. El servidor no permite que el dispositivo objetivo realice el servicio objetivo.

Por ejemplo, el servidor devuelve una respuesta de falla de verificación al dispositivo objetivo, por ejemplo, cuando el usuario ilegal usa el ordenador 13 para acceder al servidor como se describió en el ejemplo anterior, el servidor no podrá realizar el servicio.

En el método de verificación del dispositivo de esta modalidad, la huella digital del dispositivo generada de acuerdo con la información de atributo del dispositivo se transporta en el certificado de dispositivo emitido para el dispositivo, y durante la verificación del dispositivo, se permite realizar el servicio solo cuando los atributos del dispositivo coinciden con la huella digital del dispositivo en el certificado, lo que mejora la seguridad y la fiabilidad de la verificación del dispositivo.

En los ejemplos anteriores, el proceso de realizar el método de verificación del dispositivo se realiza sobre la base de que el dispositivo objetivo ha almacenado el certificado del dispositivo, y el dispositivo objetivo solo necesita transportar el certificado del dispositivo cuando envía la solicitud de verificación del dispositivo. En realidad, el servidor emite el certificado del dispositivo al dispositivo objetivo, y el dispositivo objetivo lo adquiere mediante la aplicación al servidor antes de realizar el proceso de verificación del dispositivo. La solicitud del certificado se describirá en detalle a continuación:

La Figura 3 es un diagrama de señalización esquemático de otro método de verificación de dispositivo de acuerdo con una modalidad de la presente invención, que se utiliza para describir un proceso en el que un dispositivo aplica a un servidor para un certificado y cómo el servidor genera el certificado, incluyendo las siguientes etapas:

301. El dispositivo objetivo recopila la segunda información de atributo de dispositivo y genera un par de claves pública-privada.

Cuando el servidor hace un certificado de dispositivo, los atributos de hardware del dispositivo también se establecen en el certificado y, por lo tanto, cuando el dispositivo objetivo solicita el certificado, la recopilación de los atributos de hardware del dispositivo, que puede denominarse segunda información de atributo de dispositivo, debe realizarse, de manera que puedan enviarse al servidor, permitiendo que el servidor genere el certificado del dispositivo en consecuencia.

Cabe señalar que, en esta etapa, la segunda información de atributo de dispositivo recopilada por el dispositivo objetivo puede no ser necesariamente completamente idéntica a la información de atributo en el certificado del dispositivo correspondiente; por ejemplo, suponiendo que hay tres atributos A, B y C en el certificado del dispositivo, la segunda información de atributo de dispositivo en esta etapa puede ser que el dispositivo objetivo recopile todos los atributos inherentes de hardware del dispositivo objetivo en sí, o reúna cinco atributos, o similares, que, en una palabra, pueden ser más que los atributos incluidos en el certificado del dispositivo, y los atributos en el certificado del dispositivo son algunos atributos seleccionados de los múltiples atributos; para más detalles, consulte la descripción posterior de 303. Definitivamente, la información de los atributos del segundo dispositivo también puede ser idéntica a los atributos en el certificado, por ejemplo, se recopilan tres atributos A, B y C, y los tres atributos también se establecen en el certificado cuando se hace el certificado.

Adicionalmente, además de recopilar la segunda información de atributo de dispositivo en esta etapa, el dispositivo objetivo genera además un par de claves pública-privada, que incluye una clave pública y una clave privada. La clave pública se usa para generar un certificado en 304, y la clave privada no se transmite al servidor cuando se aplica el certificado. Por ejemplo, la clave privada puede usarse para encriptar información durante la transmisión de información después de que la verificación tenga éxito, por ejemplo, la información enviada por el dispositivo objetivo al servidor es encriptada por la clave privada, y el servidor descifra la información usando la clave pública.

302. El dispositivo objetivo envía una petición de solicitud de certificado al servidor, la petición de solicitud de certificado incluye: la segunda información de atributo de dispositivo y la clave pública en el par de claves pública-privada.

Cuando el dispositivo objetivo envía la petición de solicitud de certificado al servidor, se transportará la segunda información de atributo de dispositivo recopilada en 301 y la clave pública en el par de claves pública-privada generado.

Opcionalmente, el dispositivo objetivo se aplica al servidor para el certificado del dispositivo, y la aplicación se puede iniciar en el servidor en los dos casos enumerados a continuación:

En un caso, el dispositivo objetivo descubre que no almacena un certificado de dispositivo. Dado que el servidor envía el certificado al dispositivo, el certificado se almacenará en el dispositivo y, cuando el dispositivo solicite al servidor que realice la verificación del dispositivo, el certificado se incluye en la solicitud de verificación del dispositivo; si el dispositivo objetivo confirma que no hay ningún certificado de dispositivo almacenado localmente, la verificación del dispositivo no se puede realizar posteriormente y, por lo tanto, el dispositivo objetivo iniciará una solicitud de certificado.

En otro caso, cuando el dispositivo objetivo recibe la respuesta de falla de verificación devuelta por el servidor, en otras palabras, antes de la solicitud de un certificado por el dispositivo objetivo esta vez, el dispositivo objetivo probablemente pueda usar un certificado de otro dispositivo para solicitar al servidor la verificación, y como resultado, el servidor determina que la información de atributo no coincide y devuelve un error de verificación, lo que indica que el certificado de dispositivo no es el certificado del dispositivo; por lo tanto, el dispositivo objetivo debe volver a solicitar su propio certificado de dispositivo.

303. El servidor genera una huella digital del dispositivo de acuerdo con la segunda información de atributo de dispositivo.

En esta etapa, si el número de atributos en el segundo dispositivo de información de atributos recopilados por el dispositivo objetivo es mayor que el número de piezas de información de atributos que deben basarse en el momento en que se genera la huella digital del dispositivo, los atributos se pueden seleccionar de la segunda información de atributo de dispositivo, y si la cantidad de atributos en la segunda información de atributo de dispositivo recopilados por el dispositivo objetivo es la misma que la cantidad de atributos que deben basarse en el momento en que se genera la huella digital del dispositivo, la huella digital puede generarse en función de todos de ellos.

En lo anterior, la adquisición de la segunda información de atributo de dispositivo en función de la cual se genera la huella digital del dispositivo se describe en términos del número de atributos, y suponiendo que la segunda información de atributo de dispositivo recopilada incluye: un atributo A (por ejemplo, un modelo de CPU), un atributo B (por ejemplo, un modelo de tarjeta de red), un atributo C (por ejemplo, una identificación de entrega de una tarjeta de visualización) y un atributo D (por ejemplo, un nombre de una memoria), y al adquirir atributos con base en la generación de la huella digital correspondiente, la información debe procesarse adicionalmente, por ejemplo, de la manera ilustrada siguiente:

Tabla 1 Valor hash tomado para el valor del atributo

Atributo	Valor hash
Atributo A	Valor hash del atributo A
Atributo B	Valor hash del atributo B
Atributo C	Valor hash del atributo C
Atributo D	Valor hash del atributo D

Como se muestra en la Tabla 1 anterior, la Tabla 1 muestra que el dispositivo objetivo toma valores hash para los valores de atributo de los cuatro elementos de información de atributo recopilados para garantizar la seguridad de la transmisión, y de hecho, los valores hash de los valores de atributo recopilados se transmiten al servidor. En el lado del servidor, los valores hash de estos atributos deben combinarse para formar una huella digital del dispositivo para identificar el dispositivo objetivo.

Por ejemplo: al tomar como ejemplo la selección de algunos atributos de la segunda información de atributo de dispositivo, la segunda información de atributo de dispositivo incluye múltiples valores de atributo, cada valor de atributo correspondiente a un atributo inherente de dispositivo del dispositivo objetivo, por ejemplo, los cuatro valores de atributo en la Tabla 1 anterior. El servidor selecciona un número predeterminado de valores de atributo de los cuatro atributos, por ejemplo, en esta modalidad, se seleccionan tres valores de atributo A, B y C, y estos valores de atributo se combinan para generar información de huella digital del dispositivo. La combinación se puede realizar de la siguiente manera: el atributo A, el valor hash del atributo A, el atributo B, el valor hash del atributo B, el atributo C y el valor hash del atributo C en la Tabla 1 anterior se sintetizan para tomar el hash para que sirva como información de huella digital del dispositivo. Definitivamente, también puede haber otras formas de combinación, siempre que se incluya información relacionada de los tres atributos, que no se describen en detalle.

Debe notarse que, la manera de generar la huella digital del dispositivo seleccionando algunos atributos de la segunda información de atributo de dispositivo como se describió anteriormente permitirá que la forma de verificación del dispositivo sea más confiable y segura; esto se debe a que, supongamos que el dispositivo objetivo recopila todos los atributos inherentes al hardware del mismo, el dispositivo objetivo no puede saber qué atributos serán seleccionados de ellos por el servidor para generar la huella digital del dispositivo en consecuencia, y un usuario ilegal tal como un hacker no sabe qué atributos se incluyen en el certificado del dispositivo, de manera que el hacker, incluso si él/ella tiene la intención de falsificar atributos (por ejemplo, el hacker manipula los atributos de hardware de un dispositivo legal cuando informa una solicitud de verificación del dispositivo, reemplazándolos con sus propios atributos de hardware), él/ella no sabrá qué atributos deben falsificarse, lo que aumenta la dificultad de los comportamientos ilegales del hacker, de manera que la forma de verificación tiene mayor confiabilidad.

Además, el dispositivo objetivo puede registrar los atributos inherentes de hardware que el dispositivo objetivo recopila al solicitar el certificado, de esta manera, los mismos atributos de dispositivo también se pueden recopilar cuando se solicita la verificación del dispositivo posteriormente, solo de esta manera puede estar seguro de que la información de atributos

recopilada incluye los atributos correspondientes en el certificado del dispositivo, y el servidor puede hacer coincidir y comparar los atributos.

304. El servidor genera un certificado de dispositivo que incluye la huella digital del dispositivo y la clave pública.

La siguiente Tabla 2, de manera simplificada, muestra una estructura del certificado del dispositivo generado en esta etapa:

Tabla 2 Estructura de un certificado de dispositivo

Información importante del certificado	Información extendida del certificado
Clave pública con firma	Huella digital del dispositivo

Como se muestra en la Tabla 2 anterior, el certificado del dispositivo es un certificado digital que tiene la huella digital del dispositivo incluida en la información extendida del certificado, y el certificado digital es, por ejemplo, un certificado en un formato X.509 V3. La descripción de la generación de la huella digital del dispositivo se puede encontrar en la descripción en 303. El certificado del dispositivo incluye además una clave pública con una firma de CA, y la clave pública es una clave pública en el par de claves pública-privada generada por el dispositivo objetivo. Dañar la información invalidará el certificado.

Además, cuando se genera el certificado del dispositivo, también se genera un número de serie del certificado como un atributo inherente del certificado. El lado del servidor puede registrar una correspondencia entre el certificado del dispositivo generado y la huella digital del dispositivo. Específicamente, el lado del servidor puede registrar, por ejemplo, una correspondencia entre el número de serie del certificado y la huella digital del dispositivo, y el atributo inherente del dispositivo (el atributo se refiere al atributo basado en el cual se genera la huella digital) también. Como se muestra en la siguiente Tabla 3:

Tabla 3 Correspondencia de certificado de dispositivo

Número de serie del certificado	Huella digital del dispositivo	Atributo inherente del dispositivo	Tiempo de generación del certificado	Tiempo de uso del certificado
		Atributo A	#####	****
		Atributo B		
		Atributo C		

Después de que se registra la correspondencia de la Tabla 3, cuando el servidor recibe el certificado del dispositivo incluido en la solicitud de verificación del dispositivo enviada posteriormente por el dispositivo objetivo, el certificado del dispositivo incluye el atributo de certificado del número de serie del certificado, el servidor puede buscar en la Tabla 3 de acuerdo con el número de serie del certificado, para adquirir el atributo A, el atributo B y el atributo C correspondiente a la huella digital del dispositivo correspondiente al certificado del dispositivo, y comparar los atributos con la primera información de atributo de dispositivo recopilada por el dispositivo objetivo, para determinar si coinciden entre sí.

Cabe señalar que, el número de serie del certificado también permite que la verificación del dispositivo sea más confiable; por ejemplo, suponiendo que los atributos de dos dispositivos son iguales, por ejemplo, los modelos de tarjetas de red y las identificaciones de entrega de las tarjetas de visualización son todos iguales, cuando los dos dispositivos solicitan un certificado de dispositivo, el servidor puede emitir certificados de dispositivo para los dos los dispositivos y las huellas digitales de los dispositivos que se incluyen en los certificados de los dispositivos pueden ser iguales; sin embargo, cada certificado corresponde a un número de serie de certificado único, los números de serie de los certificados de los dos dispositivos son diferentes y el servidor aún puede distinguir los dos dispositivos.

En otras palabras, al recibir la solicitud de verificación del dispositivo objetivo, el servidor no solo necesita hacer coincidir y comparar la información de atributos del dispositivo descrita en el ejemplo anterior, sino que también debe realizar una validación básica del certificado, por ejemplo, para ver si los números de serie de los certificados son los mismos, ya sea que el certificado esté dentro de un plazo de validez, si la información del certificado está completa o dañada, o similar.

305. El servidor envía el certificado del dispositivo al dispositivo objetivo.

El método de verificación del dispositivo en esta modalidad de la presente invención usa el mecanismo de combinar el certificado digital y la huella digital del dispositivo, de manera que la huella digital del dispositivo en el certificado no se puede falsificar como el certificado digital no se puede falsificar; mientras tanto, también se utiliza la singularidad del certificado digital, lo que mejora enormemente la confiabilidad de la verificación del dispositivo.

Los aparatos de verificación de dispositivo se proporcionan además de la siguiente manera, para implementar los métodos de verificación de dispositivo descritos anteriormente a través de los aparatos:

La Figura 4 es un diagrama estructural esquemático de un aparato de verificación de dispositivo de acuerdo con una modalidad de la presente invención, y el aparato puede aplicarse a un servidor, por ejemplo, un conjunto de software en un terminal de servidor. Como se muestra en la Figura 4, el aparato puede incluir: una unidad receptora de solicitud 41 y una unidad de verificación de dispositivo 42; en donde,
la unidad receptora de solicitud 41 está configurada para recibir una solicitud de verificación del dispositivo enviada por el dispositivo objetivo a verificar, la solicitud de verificación del dispositivo incluye: un certificado del dispositivo y la primera información de atributo de dispositivo del dispositivo objetivo, el certificado del dispositivo incluye una huella digital del dispositivo generada de acuerdo con la segunda información de atributo de dispositivo; y
la unidad de verificación de dispositivo 42 está configurada para, cuando se confirma de acuerdo con la huella digital del dispositivo que el certificado del dispositivo es válido, y la huella digital del dispositivo coincide con la primera información de atributo de dispositivo, determinar que el certificado del dispositivo es un certificado del dispositivo objetivo, y permitir que el dispositivo objetivo realice un servicio objetivo.

La Figura 5 es un diagrama estructural esquemático de otro aparato de verificación de dispositivo de acuerdo con una modalidad de la presente invención. Sobre la base de la estructura mostrada en la Figura 4, el aparato incluye además: una unidad de generación de certificado 43 y una unidad de envío de certificado 44; en donde,
la unidad receptora de solicitud 41 está configurada además para recibir una petición de solicitud de certificado enviada por el dispositivo objetivo, incluyendo la petición de solicitud de certificado: la segunda información de atributo de dispositivo recopilada por el dispositivo objetivo;
la unidad de generación de certificado 43 está configurada para generar la huella digital del dispositivo de acuerdo con la segunda información de atributo de dispositivo, y establecer la huella digital del dispositivo en el certificado del dispositivo generado; y
la unidad de envío de certificado 44 está configurada para enviar el certificado del dispositivo al dispositivo objetivo.

Además, la unidad de generación de certificado 43, cuando genera la huella digital del dispositivo de acuerdo con la segunda información de atributo de dispositivo, está configurada para seleccionar un número predeterminado de valores de atributo de múltiples valores de atributo incluidos en la segunda información de atributo de dispositivo, y combinar el número predeterminado de valores de atributo para generar la huella digital del dispositivo para identificar el dispositivo objetivo; cada valor de atributo correspondiente a un atributo inherente de dispositivo del dispositivo objetivo.

La Figura 6 es un diagrama estructural esquemático de otro aparato de verificación de dispositivo de acuerdo con una modalidad de la presente invención. El aparato puede aplicarse a un dispositivo objetivo, por ejemplo, un conjunto de software de terminal establecido en un lado del dispositivo objetivo. Como se muestra en la Figura 6, el aparato puede incluir: una unidad de adquisición de información 61 y una unidad de envío de solicitud 62; en donde,
la unidad de adquisición de información 61 está configurada para recopilar la primera información de atributo de dispositivo; y
la unidad de envío de solicitud 62 está configurada para enviar una solicitud de verificación de dispositivo al servidor, la solicitud de verificación de dispositivo incluye: un certificado de dispositivo y la primera información de atributo de dispositivo, el certificado de dispositivo incluye una huella digital de dispositivo generada de acuerdo con la segunda información de atributo de dispositivo, de manera que el servicio objetivo se realiza cuando el servidor determina que la huella digital del dispositivo coincide con la primera información de atributo de dispositivo.

La Figura 7 es un diagrama estructural esquemático de otro aparato de verificación de dispositivo de acuerdo con una modalidad de la presente invención. Sobre la base de la estructura mostrada en la Figura 6, el aparato incluye, además: una unidad receptora de certificados 63; en donde,
la unidad de adquisición de información 61 está configurada además para recopilar la segunda información de atributo de dispositivo;
la unidad de envío de solicitud 62 está configurada además para enviar una petición de solicitud de certificado al servidor, la petición de solicitud de certificado incluye: la segunda información de atributo de dispositivo, de manera que el servidor genera una huella digital del dispositivo de acuerdo con la segunda información de atributo de dispositivo y establece la huella digital del dispositivo en el certificado del dispositivo; y
la unidad receptora de certificado 63 está configurada para recibir el certificado de dispositivo devuelto por el servidor.

Además, la unidad de envío de solicitud 62 está configurada además para enviar la petición de solicitud de certificado cuando se confirma que no se almacena localmente ningún certificado de dispositivo, o cuando se recibe una respuesta de falla de verificación devuelta por el servidor.

Las anteriores son meramente modalidades preferidas de la presente invención, y no pretenden limitar la presente invención. La invención se define por las reivindicaciones.

REIVINDICACIONES

1. Un método de verificación de dispositivo, en donde el método de verificación de dispositivo se usa para verificar un dispositivo objetivo que solicita realizar un servicio objetivo, el método realizado por un servidor (12), el método comprende:
recibir una petición de solicitud de certificado enviada por el dispositivo objetivo, la petición de solicitud de certificado comprende la segunda información de atributo de dispositivo recopilada por el dispositivo objetivo, en donde la segunda información de atributo de dispositivo comprende: múltiples valores de atributo, cada valor de atributo correspondiente a un atributo inherente de dispositivo del dispositivo objetivo;
generar (303) una huella digital del dispositivo de acuerdo con la segunda información de atributo de dispositivo, y establecer la huella digital de dispositivo en un certificado de dispositivo generado, en donde la generación de la huella digital de dispositivo de acuerdo con la segunda información de atributo de dispositivo comprende:
seleccionar un número preestablecido de valores de atributo de los múltiples valores de atributos, en donde el número total de múltiples valores de atributos es mayor que el número preestablecido de valores de atributos, y
combinar el número preestablecido de valores de atributo para generar la huella digital del dispositivo para identificar el dispositivo objetivo;
enviar (305) el certificado del dispositivo al dispositivo objetivo;
recibir una solicitud de verificación del dispositivo enviada por el dispositivo objetivo a ser verificado, la solicitud de verificación del dispositivo que comprende el certificado del dispositivo y la primera información de atributo de dispositivo del dispositivo objetivo, y el certificado del dispositivo que comprende la huella digital del dispositivo generada de acuerdo con la segunda información de atributo de dispositivo; y
cuando se confirma de acuerdo con la huella digital del dispositivo que el certificado del dispositivo es válido y la huella digital del dispositivo coincide con la primera información de atributo de dispositivo, determinar que el certificado del dispositivo es un certificado del dispositivo objetivo y permitir que el dispositivo objetivo realice el servicio objetivo.

2. El método de la reivindicación 1, en donde la huella digital del dispositivo coincide con la primera información de atributo de dispositivo cuando:
la primera información de atributo de dispositivo coincide con la segunda información de atributo de dispositivo; o
otra huella digital del dispositivo generada de acuerdo con la primera información de atributo de dispositivo coincide con la huella digital del dispositivo en el certificado del dispositivo.

3. El método de la reivindicación 2, en donde la primera información de atributo de dispositivo coincide con la segunda información de atributo de dispositivo cuando:
los valores de atributo correspondientes en la primera información de atributo de dispositivo y la segunda información de atributo de dispositivo son todos iguales, o
una proporción del número de valores de atributo correspondientes idénticos en la primera y segunda información de atributo de dispositivo al número total de valores de atributo alcanza un umbral de proporción preestablecido.

4. Un servidor (12) que comprende un aparato de verificación de dispositivo, el aparato de verificación de dispositivo comprende:
una unidad receptora de solicitud (41) configurada para recibir una petición de solicitud de certificado enviada por un dispositivo objetivo, la petición de solicitud de certificado que comprende la segunda información de atributo de dispositivo recopilada por el dispositivo objetivo, en donde la segunda información de atributo de dispositivo comprende: múltiples valores de atributo, cada valor de atributo correspondiente a un atributo inherente de dispositivo del dispositivo objetivo;
una unidad de generación de certificado (43) configurada para generar una huella digital del dispositivo de acuerdo con la segunda información de atributo de dispositivo, y establecer la huella digital del dispositivo en un certificado de dispositivo generado, en donde en la generación de la huella digital del dispositivo, de acuerdo con la segunda información de atributo de dispositivo, la unidad de generación de certificado está configurada además para:
seleccionar un número preestablecido de valores de atributo de los múltiples valores de atributos, en donde el número total de múltiples valores de atributos es mayor que el número preestablecido de valores de atributos, y
combinar el número preestablecido de valores de atributo para generar la huella digital del dispositivo para identificar el dispositivo objetivo;
una unidad de envío de certificado (44) configurada para enviar el certificado del dispositivo al dispositivo objetivo;
la unidad receptora de solicitud (41) configurada para recibir una solicitud de verificación del dispositivo enviada por un dispositivo objetivo a ser verificado, la solicitud de verificación del dispositivo que comprende el certificado del dispositivo y la primera información de atributo del dispositivo objetivo, y el certificado del dispositivo que comprende la huella digital del dispositivo generada de acuerdo con la segunda información de atributo de dispositivo; y
una unidad de verificación de dispositivo (42) configurada para, cuando se confirma de acuerdo con la huella digital del dispositivo que el certificado del dispositivo es válido, y la huella digital del dispositivo coincide con la primera información de atributo de dispositivo, determinar que el certificado del dispositivo es un certificado del dispositivo objetivo, y permitir que el dispositivo objetivo realice un servicio objetivo.

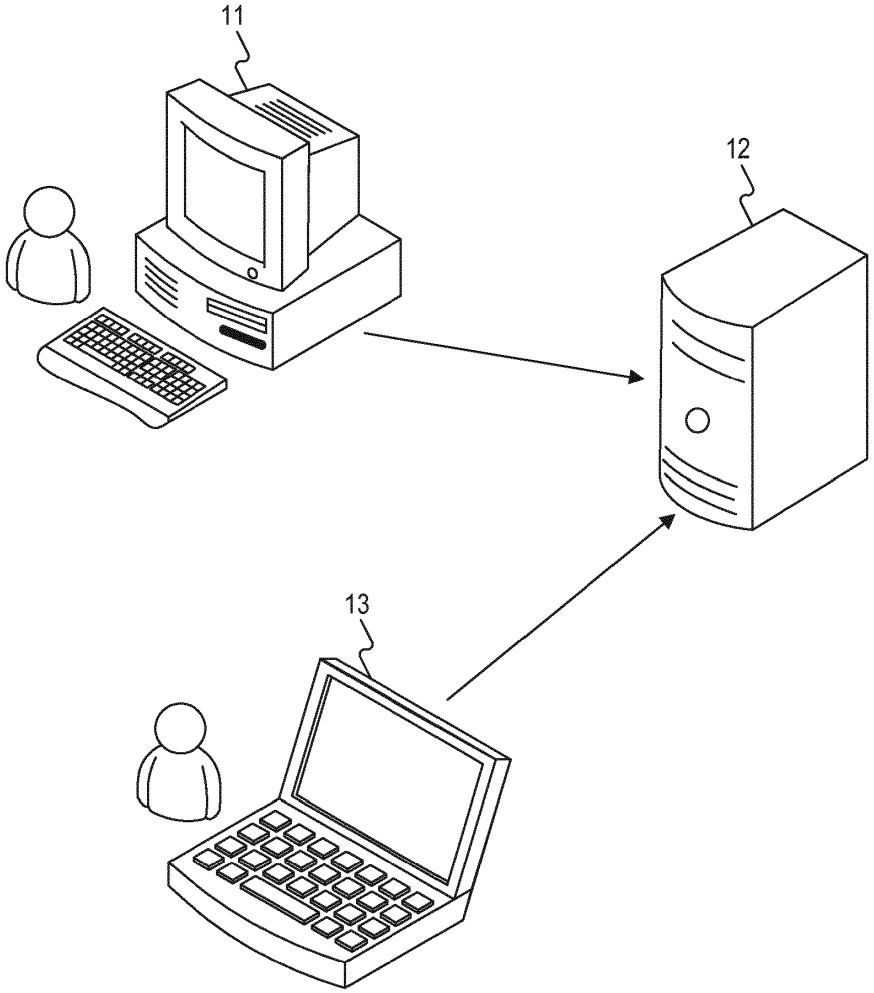

FIG. 1

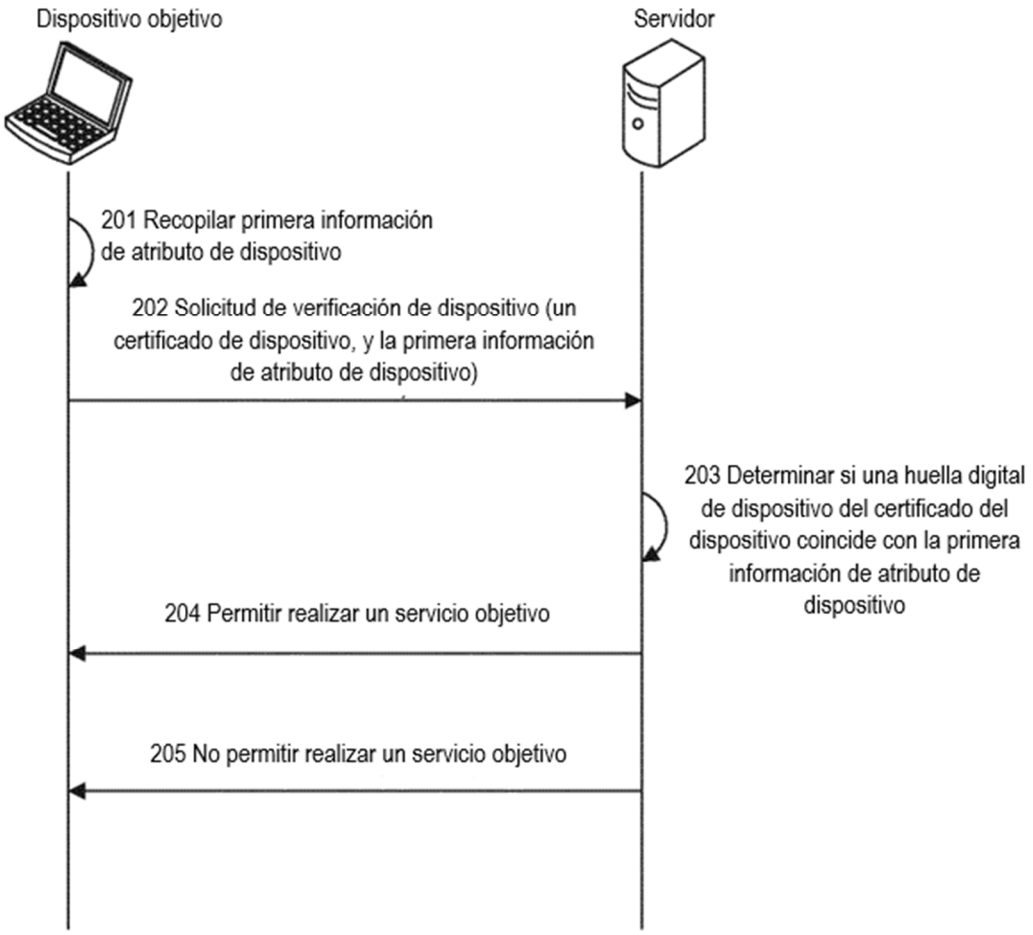
Dispositivo objetivo
Servidor
201 Recopilar primera información de atributo de dispositivo
202 Solicitud de verificación de dispositivo (un certificado de dispositivo, y la primera información de atributo de dispositivo)
203 Determinar si una huella digital de dispositivo del certificado del dispositivo coincide con la primera información de atributo de dispositivo
204 Permitir realizar un servicio objetivo
205 No permitir realizar un servicio objetivo

FIG. 2

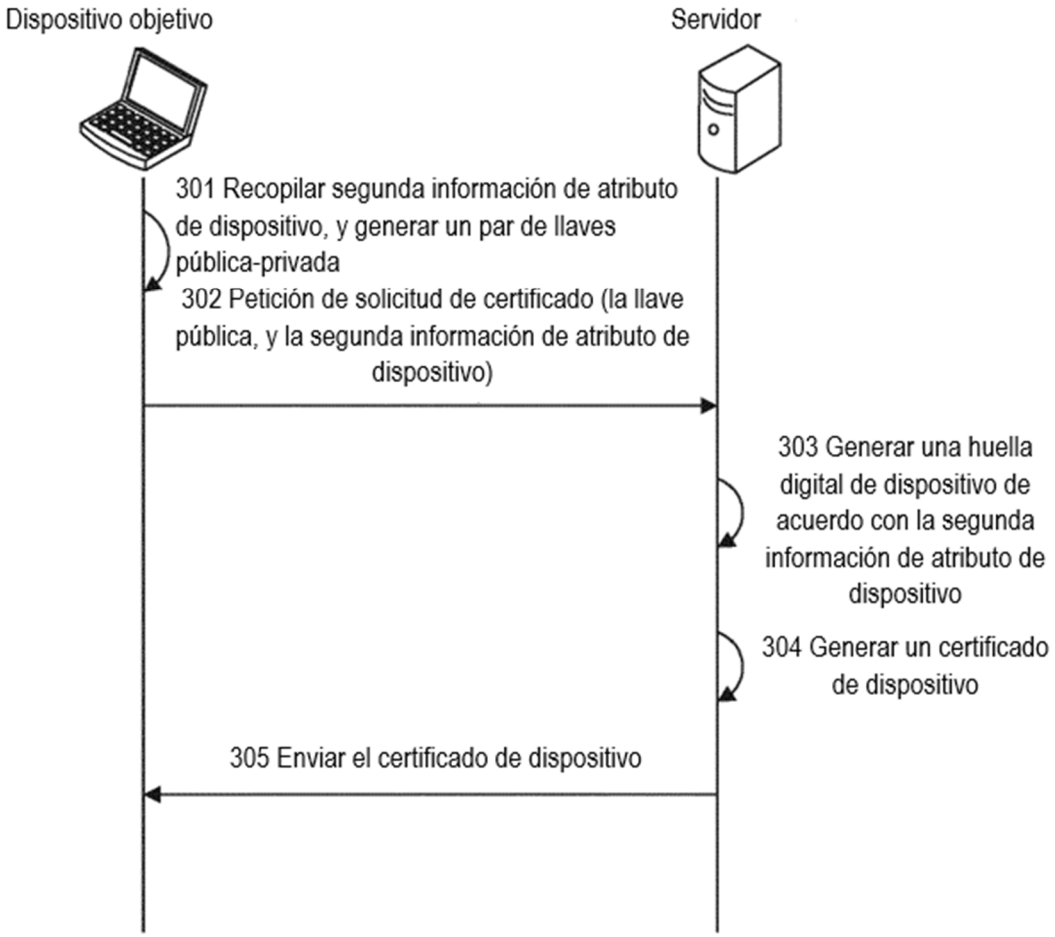
Dispositivo objetivo
Servidor
301 Recopilar segunda información de atributo de dispositivo, y generar un par de llaves pública-privada
302 Petición de solicitud de certificado (la llave pública, y la segunda información de atributo de dispositivo)
303 Generar una huella digital de dispositivo de acuerdo con la segunda información de atributo de dispositivo
304 Generar un certificado de dispositivo
305 Enviar el certificado de dispositivo

FIG. 3

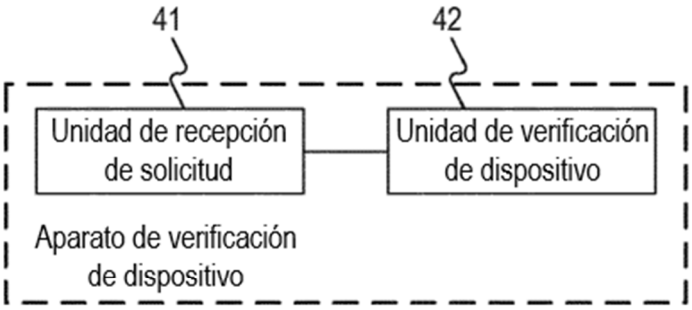
41
42
Unidad de recepción de solicitud
Unidad de verificación de dispositivo
Aparato de verificación de dispositivo

FIG. 4

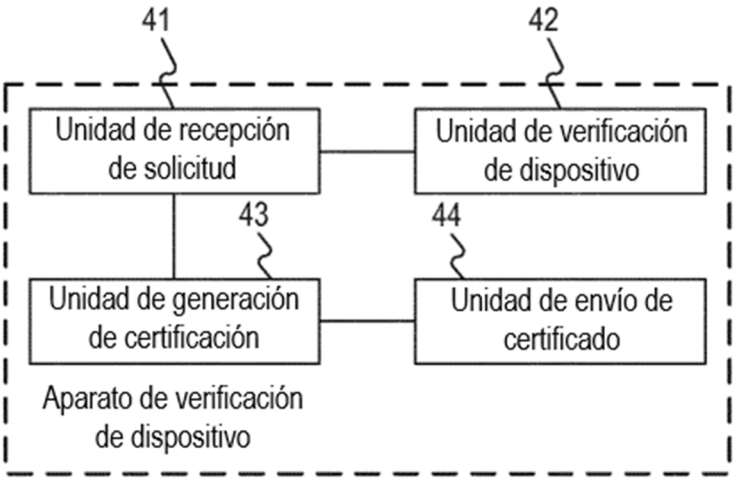
41
42
Unidad de recepción de solicitud
Unidad de verificación de dispositivo
43
44
Unidad de generación de certificación
Unidad de envío de certificado
Aparato de verificación de dispositivo

FIG. 5

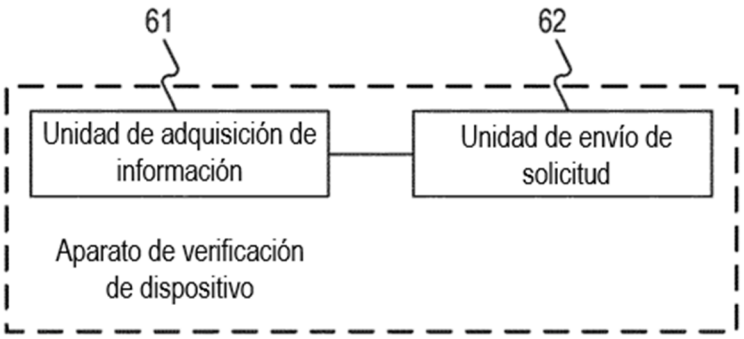
61
62
Unidad de adquisición de información
Unidad de envío de solicitud
Aparato de verificación de dispositivo

FIG. 6

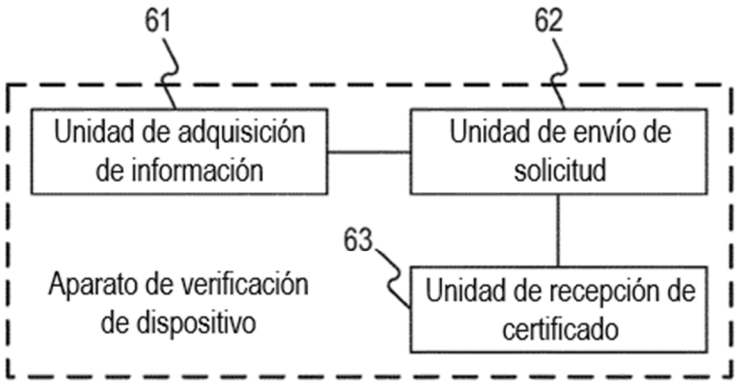
61
62
Unidad de adquisición de información
Unidad de envío de solicitud
63
Aparato de verificación de dispositivo
Unidad de recepción de certificado

FIG. 7