(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 884 169**

(51) Int. CI.:

G06Q 20/38 (2012.01)
H04L 9/08 (2006.01)
G06F 21/33 (2013.01)
H04L 9/32 (2006.01)
G06Q 20/02 (2012.01)
H04L 29/06 (2006.01)
H04W 12/06 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.10.2018 PCT/US2018/056773**

(87) Fecha y número de publicación internacional: **25.04.2019 WO19079761**

(96) Fecha de presentación y número de la solicitud europea: **19.10.2018 E 18799645 (9)**

(97) Fecha y número de publicación de la concesión europea: **19.05.2021 EP 3632036**

(54) Título: **Método y dispositivo de aplicación de certificado digital**

(30) Prioridad:

20.10.2017 CN 201710985105

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.12.2021

(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:

WEI, YAWEN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y dispositivo de aplicación de certificado digital

CAMPO TÉCNICO

La memoria descriptiva se refiere al campo de las tecnologías de seguridad y, en particular, a un método y dispositivo de aplicación de certificado digital.

ANTECEDENTES

Un certificado digital se emite normalmente por una autoridad certificadora (CA), que puede incluir una clave pública e información del propietario de la clave pública, y se puede utilizar para verificar la identidad de otra parte utilizando Internet.

Actualmente, en un proceso de aplicación de certificado digital, normalmente se necesita un archivo de solicitud de firma de certificado (CSR). Debido a que el archivo de CSR tiene una estructura de datos relativamente compleja y de gran tamaño, lo que puede consumir una cantidad significativa de recursos informáticos de un terminal. Por lo tanto, se desea una solución de aplicación de certificado práctica y ligera.

El documento US 2013/086377 A1 da a conocer un enfoque para procesar una solicitud de firma de certificado en una red de almacenamiento dispersa. Un dispositivo solicitante transmite una solicitud de firma de certificado a una unidad de gestión, en donde la solicitud de firma de certificado incluye información de certificado fija e información de certificado sugerida. La unidad de gestión reenvía la solicitud de firma de certificado a una autoridad certificadora y recibe un certificado firmado de la autoridad certificadora, en donde el certificado firmado incluye un certificado y una firma de certificación y en donde el certificado incluye la información de certificado fija y la información de certificado determinada en base a la información de certificada sugerida. La unidad de gestión interpreta la información de certificado fija del certificado firmado para identificar el dispositivo solicitante y reenviar el certificado firmado al dispositivo solicitante identificado.

La entrada de Wikipedia sobre «Certificate signing request», XP55534051, 17 de octubre de 2017, recuperada a través de https://web.archive.org/web/20171125023634/https://en.wikipedia.org/wiki/Certificate_signing_request, divulga que en los sistemas de infraestructura de clave pública una solicitud de firma de certificado es un mensaje enviado desde un solicitante a una autoridad certificadora para solicitar un certificado de identidad digital.

RESUMEN

La invención se define en las reivindicaciones independientes. Se establecen realizaciones particulares en las reivindicaciones dependientes.

La memoria descriptiva se implementa utilizando las siguientes soluciones técnicas:

Un método de aplicación de certificado digital que se aplica a un dispositivo terminal, donde el dispositivo terminal integra un elemento seguro y se carga con software de cliente, y el método incluye lo siguiente: enviar, mediante el cliente, una solicitud de aplicación de certificado digital a un servidor, de modo que el servidor genera información de aplicación en base a la solicitud de aplicación y devuelve la información de aplicación al cliente, donde la información de aplicación incluye un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación; entregar, mediante el cliente, la información de aplicación devuelta por el servidor al elemento seguro; generar, mediante el elemento seguro, un par de claves pública y privada en base a un algoritmo asimétrico, utilizar la clave privada para firmar el identificador de aplicación para obtener datos de firma del terminal, y encapsular los datos de firma del terminal y la clave pública en un formato especificado y enviar los datos de formato especificado al cliente; y enviar, mediante el cliente, los datos de formato especificado al servidor, para que el servidor envíe la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión del cliente y la información de uso del certificado a una CA después de determinar, en base a la clave pública, que se verifican los datos de firma del terminal y el identificador de aplicación.

Un método de aplicación de certificado digital, aplicado a un servidor, donde el servidor está configurado para interactuar con software de cliente cargado en un dispositivo terminal, el dispositivo terminal además integra un elemento seguro, y el método incluye generar y enviar información de aplicación a un cliente y a una CA después de recibir una solicitud de aplicación de certificado digital enviada por el cliente, donde la información de aplicación incluye un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación; recibir datos de formato especificado enviados por el cliente, donde los datos de formato especificado se obtienen después de que el elemento seguro genera un par de claves pública y privada, firma el identificador de aplicación utilizando la clave privada para obtener datos de firma de terminal y encapsula los datos de firma de terminal y la clave pública; analizar los datos de formato especificado y verificar los datos de firma del terminal en base a la clave pública, para obtener el identificador de aplicación en los datos de firma del terminal; y enviar la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión del cliente y la información de uso del certificado a la CA después de que se verifiquen

los datos de firma del terminal y el identificador de aplicación, por lo que la CA genera un certificado digital después de determinar que se verifican los datos de firma del terminal y el identificador de aplicación.

Un dispositivo de aplicación de certificado digital, aplicado a un dispositivo terminal, donde el dispositivo terminal integra además un elemento seguro, y el dispositivo incluye una unidad de envío de solicitud, configurada para enviar una solicitud de aplicación de certificado digital a un servidor, por lo que el servidor genera información de aplicación en base a la solicitud de aplicación y devuelve la información de aplicación, donde la información de aplicación incluye un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación; una unidad de entrega de información, configurada para entregar la información de aplicación devuelta por el servidor al elemento seguro, de modo que el elemento seguro genera un par de claves pública y privada en base a un algoritmo asimétrico, utiliza la clave privada para firmar el identificador de aplicación para obtener los datos de firma del terminal, y encapsula los datos de firma del terminal y la clave pública en un formato especificado y devuelve los datos de formato especificado; y una unidad de envío de datos, configurada para enviar los datos de formato especificado al servidor, de modo que el servidor envía la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión y la información de uso del certificado a una CA después de determinar, en base a la clave pública, que se verifican los datos de firma del terminal y el identificador de aplicación.

Un dispositivo de aplicación de certificado digital, aplicado a un servidor, donde el dispositivo está configurado para interactuar con software de cliente cargado en un dispositivo terminal, el dispositivo terminal integra además un elemento seguro, y el dispositivo incluye una unidad de generación de información, configurada para generar y enviar información de aplicación al cliente y a una CA, después de recibir una solicitud de aplicación de certificado digital enviada por el cliente, donde la información de aplicación incluye un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación; una unidad de recepción de datos, configurada para recibir datos de formato especificado enviados por el cliente, donde los datos de formato especificado se obtienen después de que el elemento seguro genera un par de claves pública y privada, firma el identificador de aplicación utilizando la clave privada para obtener datos de firma del terminal y encapsula los datos de firma del terminal y la clave pública; una unidad de verificación de datos, configurada para analizar los datos de formato especificado y verificar los datos de firma del terminal en base a la clave pública, para obtener el identificador de aplicación en los datos de firma del terminal; y una unidad de solicitud de certificado, configurada para enviar la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión del cliente y la información de uso del certificado a la CA después de que se verifiquen los datos de firma del terminal y el identificador de aplicación, de modo que la CA genera una certificado digital después de determinar que los datos de firma del terminal y el identificador de aplicación están verificados.

Un dispositivo de aplicación de certificado digital, aplicado a un dispositivo terminal, donde el dispositivo incluye un elemento seguro; un procesador; y una memoria configurada para almacenar una instrucción ejecutable por máquina. Al leer y ejecutar la instrucción ejecutable por máquina que está almacenada en la memoria y que corresponde a la lógica de aplicación de certificado digital, el procesador está habilitado para enviar una solicitud de aplicación de certificado digital a un servidor, de modo que el servidor genera información de aplicación en base a la solicitud de aplicación y devuelve la información de aplicación, donde la información de aplicación incluye un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación; entregar la información de aplicación devuelta por el servidor al elemento seguro, de modo que el elemento seguro genera un par de claves pública y privada en base a un algoritmo asimétrico, utiliza la clave privada para firmar el identificador de aplicación para obtener los datos de firma del terminal y encapsula los datos de firma del terminal y la clave pública en un formato especificado y devuelve los datos de formato especificado; y enviar los datos de formato especificado al servidor, de modo que el servidor envía la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión y la información de uso del certificado a una CA después de determinar, en base a la clave pública, que los datos de firma del terminal y el identificador de aplicación están verificados.

Un dispositivo de aplicación de certificado digital, aplicado a un servidor, donde el dispositivo incluye un procesador; y una memoria configurada para almacenar una instrucción ejecutable por máquina. Al leer y ejecutar la instrucción ejecutable por máquina que está almacenada en la memoria y que corresponde a la lógica de aplicación de certificado digital, el procesador está habilitado para generar y enviar información de aplicación a un cliente y a una CA después de recibir una solicitud de aplicación de certificado digital enviada por el cliente, donde la información de aplicación incluye un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación; recibir datos de formato especificado enviados por el cliente, donde los datos de formato especificado se obtienen después de que un elemento seguro genera un par de claves pública y privada, firma el identificador de aplicación utilizando la clave privada para obtener datos de firma de terminal y encapsula los datos de firma de terminal y la clave pública; analizar los datos de formato especificado y verificar los datos de firma del terminal en base a la clave pública para obtener el identificador de aplicación en los datos de firma del terminal; y enviar la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión del cliente y la información de uso del certificado a la CA después de que se verifiquen los datos de firma del terminal y el identificador de aplicación, de modo que la CA genera un certificado digital después de determinar que los datos de firma del terminal y el identificador de aplicación están verificados.

Se puede ver en la descripción anterior que en la memoria descriptiva, el terminal y el servidor pueden cooperar para generar un archivo de solicitud de firma de certificado, reducir la carga computacional del elemento seguro e implementar una solución de aplicación de certificado ligera y de alta disponibilidad. Además, el servidor y la CA

verifican por separado los datos de firma del terminal y pueden garantizar la seguridad de la aplicación de certificado digital.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La FIG. 1 es un diagrama de flujo esquemático que ilustra un método de aplicación de certificado digital, de acuerdo con una implementación de ejemplo de la memoria descriptiva;

la FIG. 2 es un diagrama de flujo esquemático que ilustra otro método de aplicación de certificado digital, de acuerdo con una implementación de ejemplo de la memoria descriptiva;

la FIG. 3 es un diagrama de flujo esquemático que ilustra otro método de aplicación de certificado digital, de acuerdo con una implementación de ejemplo de la memoria descriptiva;

la FIG. 4 es un diagrama estructural esquemático que ilustra datos especificados en un formato TLV, de acuerdo con una implementación de ejemplo de la memoria descriptiva;

la FIG. 5 es un diagrama estructural esquemático que ilustra un dispositivo terminal, de acuerdo con una implementación de ejemplo de la memoria descriptiva;

la FIG. 6 es un diagrama de bloques que ilustra un dispositivo de aplicación de certificado digital, de acuerdo con una implementación de ejemplo de la memoria descriptiva;

la FIG. 7 es un diagrama estructural esquemático que ilustra un servidor, de acuerdo con una implementación de ejemplo de la memoria descriptiva;

la FIG. 8 es un diagrama de bloques que ilustra otro dispositivo de aplicación de certificado digital, de acuerdo con una implementación de ejemplo de la memoria descriptiva; y

la FIG. 9 es un diagrama de flujo que ilustra un ejemplo de un método implementado por computadora para la aplicación de certificado digital, de acuerdo con una implementación de la presente divulgación.

DESCRIPCIÓN DE LAS IMPLEMENTACIONES

Las implementaciones de ejemplo se describen en detalle aquí, y se indica un ejemplo de las implementaciones en los dibujos adjuntos. Cuando las siguientes descripciones se refieren a los dibujos adjuntos, el mismo número en diferentes dibujos adjuntos indica el mismo elemento o uno similar, a menos que se exponga otra indicación. Las implementaciones descritas en las siguientes implementaciones de ejemplo no representan todas las implementaciones consistentes con la memoria descriptiva. Por el contrario, son solo ejemplos de dispositivos y métodos que se describen en detalle en las reivindicaciones adjuntas y que son consistentes con algunos aspectos de la memoria descriptiva.

Los términos utilizados en la memoria descriptiva son simplemente para ilustrar implementaciones específicas y no pretenden limitar la memoria descriptiva. Los términos «un», «dicho» y «el» de las formas singulares utilizadas en la memoria descriptiva y las reivindicaciones adjuntas también pretenden incluir formas plurales, a menos que se especifique claramente lo contrario en el contexto. También debe entenderse que el término "y/o" utilizado en la memoria descriptiva indica e incluye cualquiera o todas las combinaciones posibles de uno o más elementos enumerados asociados.

Debe entenderse que aunque los términos «primero», «segundo», «tercero», etc. pueden utilizarse en la memoria descriptiva para describir diversos tipos de información, la información no se limita a los términos. Estos términos sólo se utilizan para diferenciar la información del mismo tipo. Por ejemplo, sin apartarse del alcance de la memoria descriptiva, la primera información también puede denominarse segunda información y, de manera similar, la segunda información puede denominarse primera información. Dependiendo del contexto, por ejemplo, la palabra "si" utilizada aquí puede explicarse como "mientras", "cuando" o "en respuesta a determinar".

La memoria descriptiva proporciona una solución de aplicación de certificado digital, de modo que un terminal y un servidor pueden cooperar para generar un archivo de solicitud de firma de certificado generado originalmente por el terminal, ahorrando recursos computacionales del terminal.

La FIG. 1 es un diagrama de flujo esquemático que ilustra un método de aplicación de certificado digital, de acuerdo con una implementación de ejemplo de la memoria descriptiva.

El método de aplicación de certificado digital se puede aplicar a un terminal. El terminal puede ser un dispositivo electrónico tal como un teléfono móvil o un PC. El terminal normalmente carga el software de cliente (Aplicación, APP) que puede interactuar con un servidor. El software de cliente no se limita a una APP cargada de forma independiente, sino que también puede ser un navegador y demás, lo cual no está limitado en la memoria descriptiva. El terminal

además integra un elemento seguro (SE), que puede estar configurado para generar un par de claves pública y privada, e implementar una operación de cifrado, una operación de firma, etc.

Haciendo referencia a la FIG. 1, el método de aplicación de certificado digital puede incluir los siguientes pasos:

Paso 102: El cliente envía una solicitud de aplicación de certificado digital a un servidor, de modo que el servidor genera información de aplicación en base a la solicitud de aplicación y devuelve la información de aplicación al cliente, donde la información de aplicación incluye un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación.

En la presente implementación, la información de aplicación puede incluir además información tal como información de algoritmo asimétrico, información de algoritmo de firma y una marca de tiempo, lo cual no está limitada en la memoria descriptiva.

Paso 104: El cliente entrega la información de aplicación devuelta por el servidor al elemento seguro.

Paso 106: El elemento seguro genera un par de claves pública y privada en base a un algoritmo asimétrico, utiliza la clave privada para firmar el identificador de aplicación para obtener los datos de firma del terminal y encapsula los datos de firma del terminal y la clave pública en un formato especificado, y luego envía los datos de formato especificado al cliente.

En la presente implementación, cuando la información de aplicación incluye la información de algoritmo asimétrico y la información de algoritmo de firma, el elemento seguro puede generar el par de claves pública y privada en base al algoritmo asimétrico especificado en la información de aplicación, calcular un resumen del identificador de aplicación utilizando el algoritmo de firma en la información de aplicación, y firmar el resumen utilizando la clave privada para obtener los datos de firma del terminal.

En otro ejemplo, cuando el elemento seguro calcula y firma el resumen, los datos utilizados no se limitan al identificador de aplicación y pueden incluir además información tal como una longitud de clave de seguridad obtenida cuando el elemento seguro genera el par de claves pública y privada, lo cual no está limitado en la memoria descriptiva.

En la presente implementación, el formato especificado puede ser un formato de valor de longitud de tipo (TLV), etc.

Paso 108: El cliente envía los datos de formato especificado al servidor, de modo que el servidor envía la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión del cliente y la información de uso del certificado a una CA después de determinar, en base a la clave pública, que los datos de firma del terminal y el identificador de aplicación están verificados.

La FIG. 2 es un diagrama de flujo esquemático que ilustra otro método de aplicación de certificado digital, de acuerdo con una implementación de ejemplo de la memoria descriptiva.

Haciendo referencia a la FIG. 2, el método de aplicación de certificado digital se puede aplicar a un servidor. El servidor suele ser un servidor o un grupo de servidores desplegado por un proveedor de servicios de terceros. El método de aplicación de certificado digital incluye los siguientes pasos:

Paso 202: Generar y enviar información de aplicación a un cliente y a una CA después de recibir una solicitud de aplicación de certificado digital enviada por el cliente, donde la información de aplicación incluye un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación.

Paso 204: Recibir los datos de formato especificado enviados por el cliente, donde los datos de formato especificado se obtienen después de que un elemento seguro genere un par de claves pública y privada, firme el identificador de aplicación utilizando la clave privada para obtener los datos de firma del terminal y encapsule la datos de firma del terminal y la clave pública.

Paso 206: Analizar los datos de formato especificado y verificar los datos de firma del terminal en base a la clave pública, para obtener el identificador de aplicación en los datos de firma del terminal.

Paso 208: Enviar la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión del cliente y la información de uso del certificado a la CA después de verificar los datos de firma del terminal y el identificador de aplicación, de modo que la CA genera un certificado digital después de determinar que los datos de firma del terminal y el identificador de aplicación están verificados.

Se puede ver en la descripción anterior que en la presente implementación, el terminal y el servidor pueden cooperar para generar un archivo de solicitud de firma de certificado, reduciendo la carga computacional del elemento seguro e implementando una solución de aplicación de certificado ligera y de alta disponibilidad. Además, el servidor y la CA verifican los datos de firma del terminal y pueden garantizar la seguridad de la aplicación de certificado digital.

La FIG. 3 es un diagrama de flujo esquemático que ilustra otro método de aplicación de certificado digital, de acuerdo con una implementación de ejemplo de la memoria descriptiva.

Haciendo referencia a la FIG. 3, el método de aplicación de certificado digital puede incluir los siguientes pasos:

Paso 302: un cliente envía una solicitud de aplicación de certificado digital a un servidor.

En la presente implementación, al aplicar un certificado digital, un usuario de inicio de sesión basado en el cliente puede iniciar una solicitud de aplicación de certificado digital a través del cliente. Por ejemplo, la solicitud de aplicación de certificado digital se puede enviar activando una opción predeterminada.

En la presente implementación, la solicitud de aplicación de certificado digital normalmente lleva información de cuenta de usuario, tal como un ID de cuenta.

Paso 304: El servidor genera información de aplicación en base a la solicitud de aplicación y envía la información de aplicación al cliente y a una CA.

En la presente implementación, después de recibir la solicitud de aplicación de certificado digital enviada por el cliente, el servidor puede generar la información de aplicación en base a la solicitud de aplicación y enviar la información de aplicación al cliente y a la CA.

En un ejemplo, la información de aplicación puede incluir un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación. El identificador de aplicación se puede llevar en un proceso de intercambio de la aplicación de certificado digital actual y se utiliza para identificar la aplicación de certificado digital actual. Como tal, se puede enviar una nueva solicitud de certificado digital cuando el cliente envía repetidamente solicitudes de solicitud de certificado digital.

En otro ejemplo, además del identificador de aplicación, la información de aplicación puede incluir información de algoritmo asimétrico e información de algoritmo de firma. El algoritmo asimétrico normalmente es una base de algoritmo para generar un par de claves pública y privada mediante un elemento seguro, y el algoritmo de firma normalmente es una base de algoritmo para calcular un resumen mediante el elemento seguro.

Ciertamente, la información de aplicación puede incluir además otra información, tal como una marca de tiempo, lo cual no está limitado en la memoria descriptiva.

Paso 306: El cliente entrega la información de aplicación a un elemento seguro.

Paso 308: El elemento seguro genera un par de claves pública y privada.

En un ejemplo, si la información de aplicación lleva la información de algoritmo asimétrico, el elemento seguro puede generar el par de claves pública y privada en base a la información de algoritmo asimétrico. Por ejemplo, genera el par de claves pública y privada en base al algoritmo RSA que llevado en la información de aplicación.

En otro ejemplo, si la información de aplicación no lleva el algoritmo asimétrico, el elemento seguro puede generar el par de claves pública y privada en base a un algoritmo predeterminado, lo cual no está limitado en la presente implementación.

En la presente implementación, después de generar el par de claves pública y privada, el elemento seguro puede obtener además una longitud de clave de seguridad.

Paso 310: El elemento seguro utiliza la clave privada para firmar el identificador de aplicación y una longitud de clave de seguridad para obtener los datos de firma del terminal.

En base al paso 308, el elemento seguro puede utilizar el identificador de aplicación y la longitud de clave de seguridad como texto original para la firma. Puede utilizar el algoritmo de firma especificado en la información de aplicación para calcular un resumen del identificador de aplicación y la longitud de clave de seguridad, y luego utilizar la clave privada para firmar el resumen para obtener los datos de firma del terminal.

En este ejemplo, firmar la longitud de clave de seguridad es el conjunto mínimo seguro y efectivo de firmar la clave pública, de modo que se pueden ahorrar de manera efectiva los recursos de procesamiento del elemento seguro. Por otro lado, es posible calcular la clave privada solo por medio de descifrado violento para realizar la factorización en la longitud de clave de seguridad. Sin embargo, la factorización es muy difícil y actualmente no existe una solución de factorización relacionada. Por lo tanto, utilizar la longitud de clave de seguridad como el texto original de firma no afecta la seguridad de la clave privada.

En otro ejemplo, en lugar de utilizar la longitud de clave de seguridad como el texto original de firma, se puede utilizar otra información, tal como la marca de tiempo, como el texto original de firma. Ciertamente, se puede utilizar solo el identificador de aplicación como el texto original de firma, lo cual no está limitado en la memoria descriptiva.

Paso 312: El elemento seguro encapsula los datos de firma del terminal, la longitud de clave de seguridad y la clave pública en un formato especificado, y luego envía los datos de formato especificado al cliente.

En la presente implementación, el formato especificado, tal como un formato TLV, puede predeterminarse por un desarrollador, lo cual no está limitado en la memoria descriptiva.

Haciendo referencia a un diagrama esquemático del formato TLV mostrado en la FIG. 4, la información relacionada con la longitud de clave de seguridad se puede añadir al primer campo TLV a la izquierda, la información acerca de la clave pública se puede añadir al campo TLV en el medio y los datos de firma del terminal se pueden añadir al campo TLV a la derecha.

Por ejemplo, como los bits del algoritmo RSA son 1024 bits, la longitud de clave de seguridad es de 128 bytes, los datos de firma del terminal son de 128 bytes y el TLV completo contiene 265 bytes. Es mucho menor que el archivo de solicitud de firma de certificado de aproximadamente 2 KB en formato P10 en las tecnologías existentes. Como tal, la encapsulación de datos ligera se implementa en el terminal, lo que reduce la cantidad de cálculo del elemento seguro y reduce el tráfico de transmisión de red.

Paso 314: El cliente envía los datos de formato especificado al servidor.

Paso 316: El servidor analiza los datos de formato especificado y determina que los datos de firma del terminal y el identificador de aplicación están verificados.

En la presente implementación, después de recibir los datos de formato especificado, el servidor puede extraer la longitud de clave de seguridad, la clave pública y los datos de firma del terminal de los datos de formato especificado. Entonces, el servidor puede utilizar la clave pública para verificar los datos de firma del terminal y, en el proceso de verificación, obtener un identificador de aplicación y una longitud de clave de seguridad en los datos de firma del terminal; verificar si la longitud de clave de seguridad obtenida es consistente con la longitud de clave de seguridad extraída del formato especificado; en caso afirmativo, determinar que la longitud de clave de seguridad está verificada.

Si el servidor determina que los datos de firma del terminal y la longitud de clave de seguridad están verificados, el servidor puede determinar que la clave pública es segura y que los datos de formato especificado no están manipulados. Si el servidor determina además que el identificador de aplicación también está verificado, el servidor puede determinar que el cliente también está verificado, y luego puede realizar el paso 318.

Vale la pena señalar que, normalmente, la información de cuenta de usuario se lleva además en el proceso de interacción entre el cliente y el servidor. Después de recibir los datos de formato especificado, el servidor puede buscar un identificador de aplicación generado para el cliente en base a la información de cuenta y determinar si el identificador de aplicación identificado es consistente con el identificador de aplicación obtenido en el proceso de verificación de firma. En caso afirmativo, se puede determinar que el identificador de aplicación está verificado; de lo contrario, se puede determinar que el identificador de aplicación falla en la verificación. Ciertamente, en aplicaciones reales, se pueden utilizar métodos para verificar el identificador de aplicación, lo cual no está limitado en la memoria descriptiva.

En la presente implementación, si el servidor determina que los datos de firma del terminal o el identificador de aplicación fallan en la verificación, el servidor puede confirmar que la aplicación de certificado digital actual tiene un riesgo de seguridad y luego puede devolver un mensaje de error de aplicación al cliente.

Paso 318: El servidor envía la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión del cliente, la información de uso del certificado y los datos de firma del servidor a la CA.

En base al paso 316, después de determinarse que los datos de firma del terminal y el identificador de aplicación están verificados, se puede obtener la información de usuario de inicio de sesión del cliente, por ejemplo, el nombre del usuario, la dirección del usuario y el número de teléfono del usuario.

En la presente implementación, el servidor puede encapsular la clave pública llevada en los datos de formato especificado en un formato PKCS1 y enviarla junto con los datos de firma del terminal, la información de usuario, la información de uso del certificado y los datos de firma del servidor en los datos de formato especificado a la CA.

La información de uso del certificado puede incluir el propósito del certificado, la plantilla de visualización del certificado, la información de dominio autodefinida del certificado, etc.

Los datos de firma del servidor se generan después de que el servidor utilice una clave privada del servidor para firmar la información de servidor. El desarrollador puede predeterminar la información de servidor, por ejemplo, un nombre de servidor y una dirección de servidor.

Si la CA almacena una clave pública de servidor, el servidor solo puede enviar los datos de firma del servidor a la CA. Si la CA no almacena la clave pública de servidor, el servidor puede enviar la clave pública de servidor y los datos de

firma del servidor a la CA, de modo que la CA verifica los datos de firma del servidor, lo cual no está limitado en la memoria descriptiva.

Paso 320: La CA genera un certificado digital después de determinar que los datos de firma del terminal, el identificador de aplicación y los datos de firma del servidor están verificados.

En la presente implementación, después de recibir la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión del cliente, la información de uso del certificado y los datos de firma del servidor que se envían por el servidor, la CA verifica los datos de firma del terminal, el identificador de aplicación y la longitud de clave de seguridad. Por ejemplo, en base al identificador de aplicación enviado por el servidor en el paso 304, la CA verifica los datos de firma del terminal y el identificador de aplicación con referencia al método de verificación del servidor en el paso 316, y verifica la longitud de clave de seguridad en base a un tipo de algoritmo y una cantidad de bits del elemento seguro.

Por otro lado, la CA puede verificar además los datos de firma del servidor, por ejemplo, utilizando la clave pública del servidor para verificar si la firma del servidor es válida.

En la presente implementación, si la CA determina que los datos de firma del terminal, el identificador de aplicación y los datos de firma del servidor están verificados, la CA puede determinar que el elemento seguro, el cliente y el servidor son todos válidos, y luego realizar la operación de generación del certificado digital.

Puede verse en la descripción anterior que en la memoria descriptiva, se utiliza un servidor con un rendimiento de procesamiento relativamente alto para cooperar con el terminal para generar un archivo de solicitud de firma de certificado para realizar una aplicación de certificado digital, reduciendo la carga computacional del elemento seguro del terminal e implementando una solución de aplicación de certificados ligera y de alta disponibilidad. Además, el servidor verifica el elemento seguro y el cliente del terminal, y luego la CA verifica el elemento seguro y el cliente del terminal y el servidor, lo que puede garantizar además la seguridad de la aplicación del certificado digital.

Vale la pena señalar que en el paso 318, el servidor tampoco puede enviar los datos de firma del servidor a la CA, pero la CA considera que el servidor es válido por defecto y no es necesario verificar los datos de firma del servidor más adelante, lo cual no está limitado en la memoria descriptiva.

Correspondiente a la implementación del método de aplicación de certificado digital mostrado en la FIG. 1, la memoria descriptiva proporciona además una implementación de un dispositivo de aplicación de certificado digital.

La implementación del dispositivo de aplicación de certificado digital de la memoria descriptiva se puede aplicar a un dispositivo terminal, y el dispositivo terminal integra un elemento seguro. La implementación del dispositivo se puede implementar mediante software, hardware o una combinación de hardware y software. La implementación de software se utiliza como ejemplo. Como dispositivo lógico, el dispositivo se forma leyendo una instrucción de programa informático correspondiente en una memoria no volátil a una memoria mediante un procesador del dispositivo terminal donde se encuentra el dispositivo. En términos de hardware, la FIG. 5 es un diagrama estructural que ilustra el hardware del dispositivo terminal en el que se encuentra el dispositivo de aplicación de certificado digital en la memoria descriptiva. Además de un procesador, una memoria, una interfaz de red y una memoria no volátil mostrados en la FIG. 5, el dispositivo terminal en el que se encuentra el dispositivo en la implementación normalmente puede incluir otro hardware en base a una función real del dispositivo terminal. Los detalles se omiten aquí por simplicidad.

La FIG. 6 es un diagrama de bloques que ilustra un dispositivo de aplicación de certificado digital, de acuerdo con una implementación de ejemplo de la memoria descriptiva.

Haciendo referencia a la FIG. 6, el dispositivo 500 de aplicación de certificado digital se puede aplicar al dispositivo terminal mostrado en la FIG. 5, e incluye una unidad 501 de envío de solicitud, una unidad 502 de entrega de información y una unidad 503 de envío de datos.

La unidad 501 de envío de solicitud está configurada para enviar una solicitud de aplicación de certificado digital a un servidor, de modo que el servidor genera información de aplicación en base a la solicitud de aplicación y devuelve la información de aplicación, donde la información de aplicación incluye un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación.

La unidad 502 de entrega de información está configurada para entregar la información de aplicación devuelta por el servidor a un elemento seguro, de modo que el elemento seguro genera un par de claves pública y privada en base a un algoritmo asimétrico, utiliza la clave privada para firmar el identificador de aplicación para obtener datos de firma del terminal, y encapsula los datos de firma del terminal y la clave pública en un formato especificado y devuelve los datos de formato especificado.

La unidad 503 de envío de datos está configurada para enviar los datos de formato especificado al servidor, de modo que el servidor envía la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión y la información de uso del certificado a una CA después de determinar, en base a la clave pública, que los datos de firma del terminal y el identificador de aplicación están verificados.

Opcionalmente, la información de aplicación incluye además información de algoritmo asimétrico e información de algoritmo de firma. La generación, mediante el elemento seguro, de un par de claves pública y privada en base a un algoritmo asimétrico, utilizando la clave privada para firmar el identificador de aplicación para obtener datos de firma del terminal incluye generar, mediante el elemento seguro, el par de claves pública y privada en base a la información del algoritmo asimétrico en la información de aplicación, calcular la longitud de clave de seguridad y un resumen del identificador de aplicación utilizando la información de algoritmo de firma en la información de aplicación, y firmar el resumen utilizando la clave privada para obtener los datos de firma del terminal.

Opcionalmente, el formato especificado es un formato TLV.

Correspondiente a la implementación del método de aplicación de certificado digital mostrado en la FIG. 2, la memoria descriptiva proporciona además una implementación de un dispositivo de aplicación de certificado digital.

La implementación del dispositivo de aplicación de certificado digital de la memoria descriptiva se puede aplicar a un servidor, y la implementación del dispositivo se puede implementar mediante software, hardware o una combinación de hardware y software. La implementación de software se utiliza como ejemplo. Como dispositivo lógico, el dispositivo se forma leyendo una instrucción de programa informático correspondiente en una memoria no volátil a una memoria mediante un procesador de un servidor donde se encuentra el dispositivo. En términos de hardware, la FIG. 7 es un diagrama estructural que ilustra el hardware del servidor en el que se encuentra el dispositivo de aplicación de certificado digital en la memoria descriptiva. Además de un procesador, una memoria, una interfaz de red y una memoria no volátil mostrados en la FIG. 7, el servidor en el que se encuentra el dispositivo en la implementación puede incluir otro hardware en base a una función real del servidor. Los detalles se omiten por simplicidad. Los detalles se omiten por simplicidad.

La FIG. 8 es un diagrama de bloques que ilustra un dispositivo de aplicación de certificado digital, de acuerdo con una implementación de ejemplo de la memoria descriptiva.

Haciendo referencia a la FIG. 8, el dispositivo 700 de aplicación de certificado digital se puede aplicar al servidor mostrado en la FIG. 7, e incluyen una unidad 701 de generación de información, una unidad 702 de recepción de datos, una unidad 703 de verificación de datos y una unidad 704 de aplicación de certificado.

La unidad 701 de generación de información está configurada para generar y enviar información de aplicación a un cliente y a una CA, después de que se reciba una solicitud de aplicación de certificado digital enviada por el cliente, donde la información de aplicación incluye un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación.

La unidad 702 de recepción de datos está configurada para recibir datos de formato especificado enviados por el cliente, donde los datos de formato especificado se obtienen después de que un elemento seguro genere un par de claves pública y privada, firme el identificador de aplicación utilizando la clave privada para obtener los datos de firma del terminal y encapsule los datos de firma del terminal y la clave pública.

La unidad 703 de verificación de datos está configurada para analizar los datos de formato especificado y verificar los datos de firma del terminal en base a la clave pública, para obtener el identificador de aplicación en los datos de firma del terminal.

La unidad 704 de aplicación de certificado está configurada para enviar la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión del cliente y la información de uso del certificado a la CA después de que se verifiquen los datos de firma del terminal y el identificador de aplicación, de modo que la CA genera una certificado digital después de determinar que los datos de firma del terminal y el identificador de aplicación están verificados.

Opcionalmente, la información de aplicación incluye además información de algoritmo asimétrico e información de algoritmo de firma, que se utilizan por el elemento seguro para generar un par de claves pública y privada para firmar.

Opcionalmente, el servidor encapsula la clave pública en un formato PKCS 1.

Opcionalmente, la unidad 704 de aplicación de certificado está configurada además para enviar datos de firma del servidor a la CA para la verificación, cuando se verifican los datos de firma del terminal y el identificador de aplicación; donde los datos de firma del servidor se generan después de que el servidor utilice una clave privada del servidor para firmar la información de servidor.

Para un proceso de implementación de funciones y roles de cada una de las unidades en el dispositivo, se pueden hacer referencias a un proceso de implementación de los pasos correspondientes en el método anterior. Los detalles se omiten aquí por simplicidad.

Debido a que una implementación del dispositivo corresponde básicamente a una implementación del método, para las partes relacionadas, se pueden hacer referencias a descripciones relacionadas en la implementación del método. La implementación del dispositivo descrita anteriormente es simplemente un ejemplo. Las unidades descritas como

partes separadas pueden estar físicamente separadas o no, y las partes mostradas como unidades pueden ser unidades físicas o no, pueden estar ubicadas en una posición o pueden estar distribuidas en una pluralidad de unidades de red. Algunos o todos los módulos pueden seleccionarse en base a los requisitos reales para lograr los objetivos de las soluciones de la memoria descriptiva. Un experto en la técnica puede comprender e implementar sin esfuerzos creativos la memoria descriptiva.

El sistema, dispositivo, módulo o unidad ilustrado en las implementaciones anteriores puede implementarse utilizando un chip informático o una entidad, o puede implementarse utilizando un producto que tenga cierta función. Un dispositivo de implementación típico es una computadora, y la computadora puede ser una computadora personal, una computadora portátil, un teléfono móvil, un teléfono con cámara, un teléfono inteligente, un asistente digital personal, un reproductor multimedia, un dispositivo de navegación, un dispositivo de recepción y envío de correo electrónico, una consola de juegos, una computadora tableta, un dispositivo ponible o cualquier combinación de estos dispositivos.

Correspondiente a la implementación del método de aplicación de certificado digital mostrado en la FIG. 1, la memoria descriptiva proporciona además un dispositivo de aplicación de certificado digital, y el dispositivo de aplicación de certificado digital incluye un elemento seguro, un procesador y una memoria configurada para almacenar una instrucción ejecutable por máquina. El procesador y la memoria normalmente están conectados entre sí utilizando un bus interno. En otras implementaciones posibles, el dispositivo puede incluir además una interfaz externa para comunicarse con otros dispositivos o componentes.

En la presente implementación, al leer y ejecutar la instrucción ejecutable por máquina que está almacenada en la memoria y que corresponde a la lógica de aplicación de certificado digital, el procesador está habilitado para enviar una solicitud de aplicación de certificado digital a un servidor, de modo que el servidor genera información de aplicación en base a la solicitud de aplicación y devuelve la información de aplicación, donde la información de aplicación incluye un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación; entregar la información de aplicación devuelta por el servidor al elemento seguro, de modo que el elemento seguro genera un par de claves pública y privada en base a un algoritmo asimétrico, utiliza la clave privada para firmar el identificador de aplicación para obtener los datos de firma del terminal y encapsula los datos de firma del terminal y la clave pública en un formato especificado y devuelve los datos de formato especificado; y enviar los datos de formato especificado al servidor, de modo que el servidor envía la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión y la información de uso del certificado a una CA después de determinar, en base a la clave pública, que los datos de firma del terminal y el identificador de aplicación están verificados.

Correspondiente a la implementación del método de aplicación de certificado digital mostrado en la FIG. 2, la memoria descriptiva proporciona además un dispositivo de aplicación de certificado digital, y el dispositivo de aplicación de certificado digital incluye un procesador y una memoria configurada para almacenar una instrucción ejecutable por máquina. El procesador y la memoria normalmente están conectados entre sí utilizando un bus interno. En otras implementaciones posibles, el dispositivo puede incluir además una interfaz externa para comunicarse con otros dispositivos o componentes.

En la presente implementación, al leer y ejecutar la instrucción ejecutable por máquina que está almacenada en la memoria y que corresponde a la lógica de aplicación de certificado digital, el procesador está habilitado para generar y enviar información de aplicación a un cliente y a una CA después de recibir una solicitud de aplicación de certificado digital enviada por el cliente, donde la información de aplicación incluye un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación; recibir datos de formato especificado enviados por el cliente, donde los datos de formato especificado se obtienen después de que un elemento seguro genera un par de claves pública y privada, firma el identificador de aplicación utilizando la clave privada para obtener datos de firma de terminal y encapsula los datos de firma de terminal y la clave pública; analizar los datos de formato especificado y verificar los datos de firma del terminal en base a la clave pública para obtener el identificador de aplicación en los datos de firma del terminal; y enviar la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión del cliente y la información de uso del certificado a la CA después de que se verifiquen los datos de firma del terminal y el identificador de aplicación, de modo que la CA genera un certificado digital después de determinar que los datos de firma del terminal y el identificador de aplicación están verificados.

Correspondiente a la implementación del método de aplicación de certificado digital mostrado en la FIG. 1, la memoria descriptiva proporciona además un medio de almacenamiento legible por computadora. El medio de almacenamiento legible por computadora almacena un programa informático, y cuando el programa se ejecuta por un procesador, se implementan los siguientes pasos: enviar una solicitud de aplicación de certificado digital a un servidor, de modo que el servidor genera información de aplicación en base a la solicitud de aplicación y devuelve la información de aplicación, donde la información de aplicación incluye un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación; entregar la información de aplicación devuelta por el servidor a un elemento seguro, de modo que el elemento seguro genera un par de claves pública y privada en base a un algoritmo asimétrico, utiliza la clave privada para firmar el identificador de aplicación para obtener los datos de firma del terminal y encapsula los datos de firma del terminal y la clave pública en un formato especificado y devuelve los datos de formato especificado; y enviar los datos de formato especificado al servidor, de modo que el servidor envía la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión y la información de uso del certificado a una CA después de determinar, en base a la clave pública, que los datos de firma del terminal y el identificador de aplicación están verificados.

Correspondiente a la implementación del método de aplicación de certificado digital mostrado en la FIG. 2, la memoria descriptiva proporciona además un medio de almacenamiento legible por computadora. El medio de almacenamiento legible por computadora almacena un programa informático, y cuando el programa se ejecuta por un procesador, se implementan los siguientes pasos: generar y enviar información de aplicación a un cliente y a una CA después de recibir una solicitud de aplicación de certificado digital enviada por el cliente, donde la información de aplicación incluye un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación; recibir datos de formato especificado enviados por el cliente, donde los datos de formato especificado se obtienen después de que un elemento seguro genera un par de claves pública y privada, firma el identificador de aplicación utilizando la clave privada para obtener datos de firma del terminal y encapsula los datos de firma del terminal y la clave pública; analizar los datos de formato especificado y verificar los datos de firma del terminal en base a la clave pública, para obtener el identificador de aplicación en los datos de firma del terminal; y enviar la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión del cliente y la información de uso del certificado a la CA después de que se verifiquen los datos de firma del terminal y el identificador de aplicación, de modo que la CA genera un certificado digital después de determinar que los datos de firma del terminal y el identificador de aplicación están verificados.

Las implementaciones específicas de la memoria descriptiva se describen arriba. Otras implementaciones caen dentro del alcance de las reivindicaciones adjuntas. En algunas situaciones, las acciones o pasos descritos en las reivindicaciones se pueden realizar en un orden diferente al orden en la implementación y aún se pueden lograr los resultados deseados. Además, el proceso representado en los dibujos adjuntos no requiere necesariamente un orden de ejecución particular para lograr los resultados deseados. En algunas implementaciones, el procesamiento en paralelo y multitarea puede ser ventajoso.

Las descripciones anteriores son simplemente implementaciones de ejemplo de la memoria descriptiva, pero no pretenden limitar la memoria descriptiva. Cualquier modificación, reemplazo equivalente o mejora realizada sin apartarse del espíritu y principio de la memoria descriptiva debe caer dentro del alcance de protección de la memoria descriptiva.

La FIG. 9 es un diagrama de flujo que ilustra un ejemplo de un método 900 implementado por computadora para la aplicación de certificado digital de acuerdo con una implementación de la presente divulgación. Para mayor claridad de presentación, la descripción que sigue describe generalmente el método 900 en el contexto de las otras figuras en esta descripción. Sin embargo, se entenderá que el método 900 se puede realizar, por ejemplo, mediante cualquier sistema, entorno, software y hardware, o una combinación de sistemas, entornos, software y hardware, según sea apropiado. En algunas implementaciones, diversas etapas del método 900 se pueden ejecutar en paralelo, en combinación, en bucles, o en cualquier orden.

En 902, la información de aplicación se recibe por un cliente y desde un servidor, y la información de aplicación incluye un identificador de aplicación correspondiente a una solicitud de aplicación de certificado digital transmitida por el cliente al servidor. En algunas implementaciones, el servidor genera la información de aplicación en base a la solicitud de aplicación del certificado digital.

En algunas implementaciones, la información de aplicación incluye además información de algoritmo asimétrico, información de algoritmo de firma y una marca de tiempo. En algunas implementaciones, los datos de formato especificado se generan calculando una longitud de clave de seguridad y un resumen del identificador de aplicación utilizando la información de algoritmo de firma. Desde el 902, el método 900 pasa al 904.

En 904, se entrega la información de aplicación a un elemento seguro asociado con el cliente. Desde el 904, el método 900 pasa al 906.

En 906, el elemento seguro genera un par de claves pública y privada. En algunas implementaciones, los datos de formato especificado se generan en un elemento seguro mediante una serie de pasos que incluyen, recibir mediante el elemento seguro y el cliente, la información de aplicación; generar un par de claves pública y privada en base a un algoritmo asimétrico; calcular una longitud de clave de seguridad y un resumen del identificador de aplicación utilizando la información de algoritmo de firma; firmar el resumen utilizando la clave privada para obtener los datos de firma del terminal; y encapsular los datos de firma del terminal y la clave pública en el formato especificado. Desde el 906, el método 900 pasa al 908.

En 908, el identificador de aplicación se firma utilizando la clave privada para generar datos de firma del terminal. Desde el 908, el método 900 pasa al 910.

En 910, los datos de formato especificado se generan encapsulando los datos de firma del terminal y la clave pública en los datos de formato especificado. Desde el 910, el método 900 pasa al 912.

En 912, los datos de formato especificado se transmiten desde el elemento seguro al cliente. Desde el 912, el método 900 pasa al 914.

En 914, el cliente transmite los datos de formato especificado al servidor. En algunas implementaciones, lo implementado por computadora además realiza una serie de pasos que incluyen, determinar mediante el servidor y

en base a la clave pública, que los datos de firma del terminal y el identificador de aplicación recibidos están verificados; y enviar mediante el servidor la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión del cliente y la información de uso del certificado a una autoridad certificadora (CA). En algunas implementaciones, tales implementaciones incluyen además la generación mediante la CA de un certificado digital. En algunas implementaciones, los datos de firma del servidor se generan por el servidor utilizando una clave privada del servidor para firmar la información de servidor, y la información de servidor está predeterminada por un desarrollador. Después de 914, el método 900 se puede detener.

Las implementaciones de la presente solicitud pueden resolver problemas técnicos en la verificación de identidad de usuario en Internet mediante certificado digital. Tradicionalmente, en un proceso de aplicación de certificado digital, normalmente se necesita un archivo de solicitud de firma de certificado (CSR). Debido a que el archivo de CSR tiene una estructura de datos compleja y un gran tamaño, lo que resulta en un consumo significativo de recursos computacionales de un terminal. Por lo tanto, se desea una solución de aplicación de certificado práctica y ligera.

La implementación de la presente solicitud proporciona métodos y aparatos para mejorar la velocidad y la eficiencia en la generación de un certificado digital que se utiliza para la verificación de identidad en Internet. De acuerdo con estas implementaciones, el terminal y el servidor pueden cooperar para generar un archivo de solicitud de firma de certificado, reduciendo la carga computacional del elemento seguro e implementando una solución de aplicación de certificado ligera y de alta disponibilidad. Por ejemplo, en un proceso de intercambio de la presente aplicación de certificado digital, se puede llevar un identificador de aplicación en dicho proceso y se puede utilizar para identificar la presente aplicación de certificado digital. Como tal, se puede enviar una nueva solicitud de certificado digital cuando el cliente envía repetidamente solicitudes de solicitud de certificado digital. Además, el servidor y la CA verifican los datos de firma del terminal y pueden garantizar la seguridad de la aplicación de certificado digital. Por ejemplo, el método de verificación utilizado en la presente divulgación requiere firmar la longitud de clave de seguridad, que es el conjunto mínimo seguro y efectivo de firma de la clave pública. Por lo tanto, los recursos de procesamiento del elemento seguro se pueden ahorrar de manera efectiva. Por otro lado, es posible calcular la clave privada solo por medio de descifrado violento para realizar la factorización en la longitud de clave de seguridad. Sin embargo, la factorización es muy difícil y actualmente no existe una solución de factorización relacionada. Por lo tanto, utilizar la longitud de clave de seguridad, como el texto original de firma no afecta la seguridad de la clave privada.

Las realizaciones y las operaciones descritas en esta memoria descriptiva pueden implementarse en circuitería electrónica digital, o en software, firmware o hardware informático, incluidas las estructuras descritas en esta memoria descriptiva o en combinaciones de una o más de ellas. Las operaciones se pueden implementar como operaciones realizadas por un aparato de procesamiento de datos sobre datos almacenados en uno o más dispositivos de almacenamiento legibles por computadora o recibidos de otras fuentes. Un aparato de procesamiento de datos, computadora o dispositivo informático puede abarcar aparatos, dispositivos y máquinas para el procesamiento de datos, incluyendo a modo de ejemplo un procesador programable, una computadora, un sistema en chip, o múltiples o combinaciones de los anteriores. El aparato puede incluir circuitería lógica de propósito especial, por ejemplo, una unidad central de procesamiento (CPU), una matriz de puertas programables en campo (FPGA) o un circuito integrado de aplicación específica (ASIC). El aparato también puede incluir código que crea un entorno de ejecución para el programa informático en cuestión, por ejemplo, código que constituye el firmware del procesador, una pila de protocolos, un sistema de gestión de bases de datos, un sistema operativo (por ejemplo, un sistema operativo o una combinación de sistemas operativos), un entorno de ejecución multiplataforma, una máquina virtual, o una combinación de uno o más de ellos. El aparato y el entorno de ejecución pueden realizar diversas infraestructuras de modelos de computación diferentes, tales como servicios web, computación distribuida e infraestructuras de computación en malla.

Un programa informático (también conocido, por ejemplo, como programa, software, aplicación de software, módulo de software, unidad de software, secuencia de comandos o código) se puede escribir en cualquier forma de lenguaje de programación, incluyendo lenguajes compilados o interpretados, lenguajes declarativos o procedimentales, y se puede implementar en cualquier forma, incluyendo como un programa independiente o como un módulo, componente, subrutina, objeto u otra unidad adecuada para su utilización en un entorno informático. Un programa se puede almacenar en una parte de un archivo que contiene otros programas o datos (por ejemplo, una o más secuencias de comandos almacenadas en un documento de lenguaje de marcado), en un único archivo dedicado al programa en cuestión, o en múltiples archivos coordinados (por ejemplo, archivos que almacenan uno o más módulos, subprogramas o partes de código). Un programa informático se puede ejecutar en una computadora o en múltiples computadoras ubicadas en un mismo sitio o distribuidas en múltiples sitios e interconectadas por una red de comunicaciones.

Los procesadores para la ejecución de un programa informático incluyen, a modo de ejemplo, tanto los microprocesadores de propósito general como los de propósito especial, y uno o más procesadores de cualquier clase de computadora digital. Por lo general, un procesador recibirá instrucciones y datos de una memoria de solo lectura, de una memoria de acceso aleatorio o de ambas. Los elementos esenciales de una computadora son un procesador para realizar acciones de acuerdo con las instrucciones y uno o más dispositivos de memoria para almacenar instrucciones y datos. Por lo general, una computadora también incluirá, o se acoplará de forma operativa para recibir datos desde o transferir datos a, o ambos, uno o más dispositivos de almacenamiento masivo para almacenar datos. Una computadora se puede integrar en otro dispositivo, por ejemplo, un dispositivo móvil, un asistente digital personal (PDA), una consola de juegos, un receptor del sistema de posicionamiento global (GPS) o un dispositivo de

almacenamiento portátil. Los dispositivos adecuados para almacenar las instrucciones y los datos del programa informático incluyen memorias no volátiles, medios y dispositivos de memoria, incluyendo, a modo de ejemplo, dispositivos de memoria de semiconductores, discos magnéticos y discos magneto-ópticos. El procesador y la memoria se pueden complementar por, o incorporar en, circuitería lógica de propósito especial.

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

Para posibilitar la interacción con un usuario, las realizaciones se pueden implementar en una computadora que tenga un dispositivo de visualización y un dispositivo de entrada, por ejemplo, una pantalla de cristal líquido (LCD) o un diodo orgánico de emisión de luz (OLED)/realidad virtual (VR)/realidad aumentada (AR) para mostrar información al usuario y una pantalla táctil, un teclado y un dispositivo señalador mediante el cual el usuario pueda proporcionar información al ordenador. También se pueden utilizar otras clases de dispositivos para posibilitar la interacción con el usuario; por ejemplo, la retroalimentación que se proporciona al usuario puede ser cualquier forma de retroalimentación sensorial, por ejemplo, retroalimentación visual, auditiva o táctil; y la entrada del usuario se puede recibir de cualquier forma, incluyendo entrada acústica, verbal o táctil. Además, una computadora puede interactuar con un usuario enviando documentos a y recibiendo documentos de un dispositivo utilizado por el usuario; por ejemplo, enviando páginas web a un navegador web en un dispositivo cliente del usuario en respuesta a las solicitudes recibidas del navegador web.

Las realizaciones se pueden implementar utilizando dispositivos informáticos interconectados por cualquier forma o medio de comunicación de datos digital cableado o inalámbrico (o una combinación de los mismos), por ejemplo, una red de comunicaciones. Ejemplos de dispositivos interconectados son un cliente y un servidor generalmente remotos entre sí que suelen interactuar a través de una red de comunicaciones. Un cliente, por ejemplo, un dispositivo móvil, puede realizar transacciones por sí mismo, con un servidor, o a través de un servidor, por ejemplo, realizando transacciones de compra, venta, pago, regalo, envío o préstamo, o autorizando las mismas. Dichas transacciones se pueden realizar en tiempo real, de tal manera que una acción y una respuesta sean temporalmente próximas; por ejemplo, un individuo percibe que la acción y la respuesta se producen, en esencia, de forma simultánea, la diferencia de tiempo para una respuesta que sigue a la acción del individuo es inferior a 1 milisegundo (ms) o inferior a 1 segundo (s), o la respuesta es sin retraso intencionado teniendo en cuenta las limitaciones de procesamiento del sistema.

Los ejemplos de redes de comunicaciones incluyen, pero no limitan una red de área local (LAN), una red de acceso de radio (RAN), una red de área metropolitana (MAN) y una red de área amplia (WAN). La red de comunicaciones puede incluir la totalidad o una parte de Internet, otra red de comunicaciones o una combinación de redes de comunicaciones. La información se puede transmitir en la red de comunicaciones de acuerdo con diversos protocolos y estándares, incluidos evolución a largo plazo (LTE), 5G, IEEE 802, Protocolo de Internet (IP) u otros protocolos o combinaciones de protocolos. La red de comunicaciones puede transmitir voz, vídeo, datos biométricos o de autenticación, u otra información entre los dispositivos informáticos conectados.

Las características descritas como implementaciones separadas se pueden implementar, en combinación, en una única implementación, mientras que las características descritas como una única implementación se pueden implementar en múltiples implementaciones, por separado, o en cualquier subcombinación adecuada. Las operaciones descritas y reivindicadas en un orden particular no se deben entender como que se requiere ese orden particular, ni que se deban realizar todas las operaciones ilustradas (algunas operaciones pueden ser opcionales). Según el caso, se puede realizar la multitarea o el procesamiento en paralelo (o una combinación de multitarea y procesamiento en paralelo).

REIVINDICACIONES

1. Un método de aplicación de certificado digital, en donde un dispositivo cliente integra un elemento seguro y se carga con el software de cliente, el método que comprende:

enviar, mediante el dispositivo cliente, una solicitud de aplicación de certificado digital a un servidor, en donde el servidor genera información de aplicación en base a la solicitud de aplicación y devuelve la información de aplicación al dispositivo cliente y a una autoridad certificadora, y en donde la información de aplicación comprende un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación;

entregar, mediante el dispositivo cliente, la información de aplicación devuelta por el servidor al elemento seguro;

generar, mediante el elemento seguro, un par de claves pública y privada en base a un algoritmo asimétrico;

firmar, mediante el elemento seguro, el identificador de aplicación utilizando la clave privada para obtener datos de firma del terminal;

encapsular, mediante el elemento seguro, los datos de firma del terminal y la clave pública en un formato especificado y enviar los datos de formato especificado al dispositivo cliente; y

enviar, mediante el dispositivo cliente, los datos de formato especificado al servidor, en donde el servidor envía la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión del cliente y la información de uso del certificado a la autoridad certificadora después de determinar, en base a la clave pública, que se verifican los datos de firma del terminal y el identificador de aplicación, en donde la autoridad certificadora genera un certificado digital después de determinar que los datos de firma del terminal y el identificador de aplicación están verificados.

2. El método de acuerdo con la reivindicación 1, en donde:

la información de aplicación comprende además información de algoritmo asimétrico e información de algoritmo de firma; y

generar, mediante el elemento seguro, un par de claves pública y privada en base a un algoritmo asimétrico y firmar, mediante el elemento seguro, el identificador de aplicación utilizando la clave privada para obtener datos de firma del terminal comprende:

generar, mediante el elemento seguro, el par de claves pública y privada en base a la información de algoritmo asimétrico en la información de aplicación,

calcular una longitud de clave de seguridad y un resumen del identificador de aplicación utilizando la información de algoritmo de firma en la información de aplicación, y

firmar el resumen utilizando la clave privada para obtener los datos de firma del terminal.

3. El método de acuerdo con la reivindicación 1, en donde el formato especificado es un formato de valor de longitud de tipo.

4. Un método de aplicación de certificado digital, en donde un servidor está configurado para interactuar con software de cliente cargado en un dispositivo cliente, en donde el dispositivo cliente integra además un elemento seguro, el método que comprende:

después de recibir una solicitud de aplicación de certificado digital enviada por el dispositivo cliente, generar información de aplicación y enviar la información de aplicación al dispositivo cliente y a una autoridad certificadora, en donde la información de aplicación comprende un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación;

recibir datos de formato especificado enviados por el dispositivo cliente, en donde los datos de formato especificado se obtienen después de que el elemento seguro genera un par de claves pública y privada, firma el identificador de aplicación utilizando la clave privada para obtener datos de firma del terminal y encapsula los datos de firma del terminal y la clave pública;

analizar los datos de formato especificado y verificar los datos de firma del terminal en base a la clave pública para obtener el identificador de aplicación en los datos de firma del terminal; y

enviar la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión del cliente y la información de uso del certificado a la autoridad certificadora después de que se verifiquen los datos de firma del terminal y el identificador de aplicación, en donde la autoridad certificadora genera un certificado digital después de determinar que los datos de firma del terminal y el identificador de aplicación están verificados.

5. El método de acuerdo con la reivindicación 4, en donde la información de aplicación comprende además información de algoritmo asimétrico e información de algoritmo de firma, en donde la información de algoritmo asimétrico y la información de algoritmo de firma se utilizan por el elemento seguro para generar el par de claves pública y privada para la firma.

6. El método de acuerdo con la reivindicación 4, en donde el servidor encapsula la clave pública en un formato PKCS 1.

7. El método de acuerdo con la reivindicación 4, que comprende, además:

enviar datos de firma del servidor a la autoridad certificadora para verificación cuando los datos de firma del terminal y el identificador de aplicación están verificados; en donde

los datos de firma del servidor se generan después de que el servidor utiliza una clave privada del servidor para firmar la información de servidor.

8. El método de acuerdo con la reivindicación 4, en donde el identificador de aplicación se lleva en un proceso de intercambio de la aplicación de certificado digital y se utiliza para identificar la aplicación de certificado digital actual.

9. El método de acuerdo con la reivindicación 4, en donde el método comprende además, después de recibir los datos de formato especificado enviados por el dispositivo cliente:

extraer, mediante el servidor, la longitud de clave de seguridad, la clave pública y los datos de firma del terminal de los datos de formato especificado;

verificar los datos de firma del terminal utilizando la clave pública;

obtener una longitud de clave de seguridad en los datos de firma del terminal;

verificar si la longitud de clave de seguridad obtenida es consistente con la longitud de clave de seguridad extraída del formato especificado; y

en caso afirmativo, determinar que la longitud de clave de seguridad está verificada.

10. El método de acuerdo con la reivindicación 9, que comprende además, en respuesta a verificar los datos de firma del terminal y determinar que la longitud de clave de seguridad está verificada, determinar que la clave pública es segura y el formato especificado no está alterado.

11. El método de acuerdo con la reivindicación 10, que comprende además determinar si el identificador de aplicación está verificado y, en respuesta determinar que el identificador de aplicación está verificado, determinar que el dispositivo cliente está verificado.

12. El método de acuerdo con la reivindicación 4 o la reivindicación 11, en donde, en respuesta determinar que los datos de firma del terminal o el identificador de aplicación fallan en la verificación, el método que comprende, además:

confirmar que la aplicación de certificado digital tiene un riesgo de seguridad; y

devolver un mensaje de error de aplicación al dispositivo cliente.

13. Un sistema de aplicación de certificado digital, que comprende un certificado de cliente, un servidor y una autoridad certificadora, en donde el certificado de cliente, el servidor y la autoridad certificadora están configurados para realizar el método de acuerdo con una cualquiera de las reivindicaciones 1 a 12.

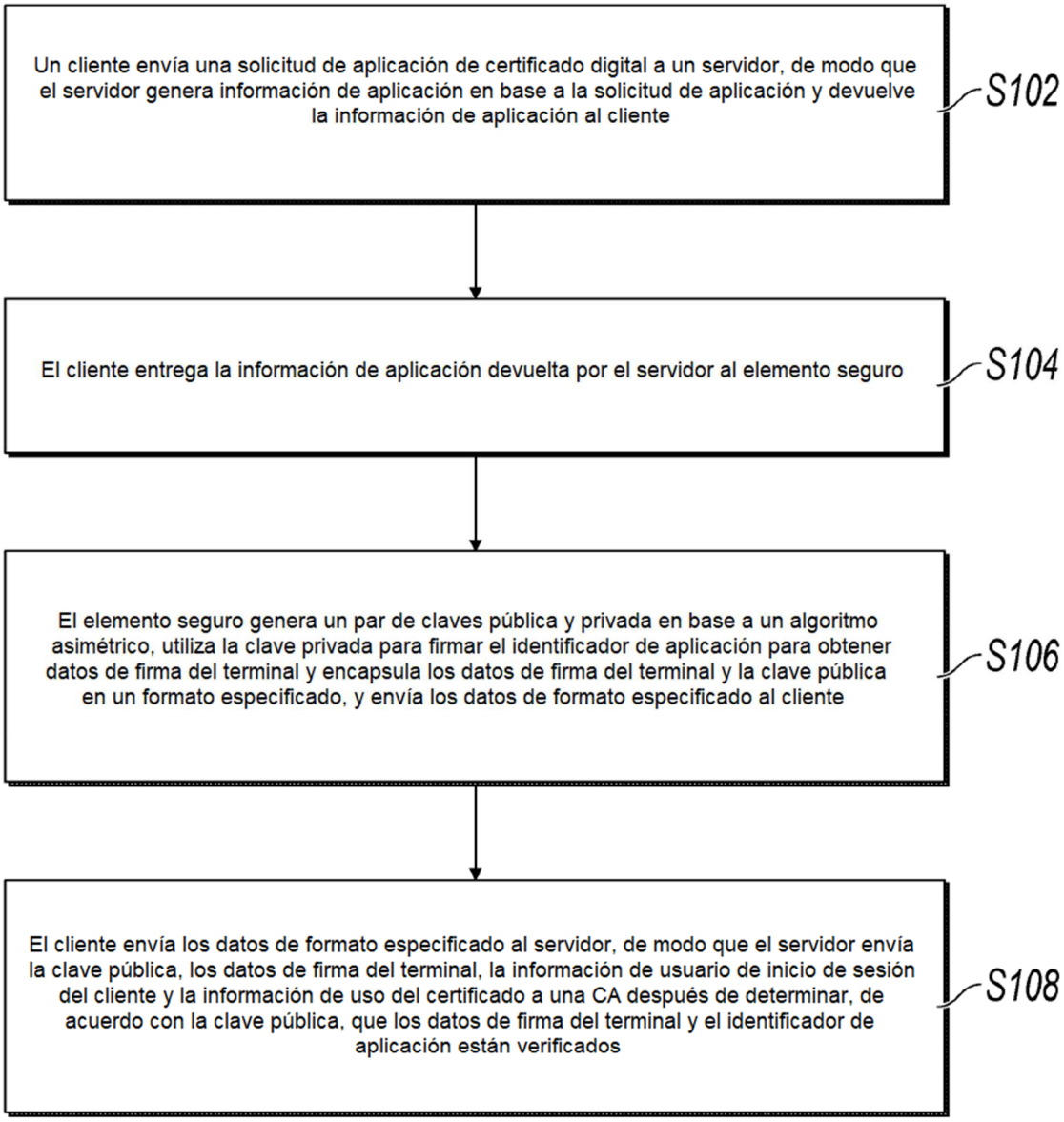
Un cliente envía una solicitud de aplicación de certificado digital a un servidor, de modo que el servidor genera información de aplicación en base a la solicitud de aplicación y devuelve la información de aplicación al cliente
S102
El cliente entrega la información de aplicación devuelta por el servidor al elemento seguro
S104
El elemento seguro genera un par de claves pública y privada en base a un algoritmo asimétrico, utiliza la clave privada para firmar el identificador de aplicación para obtener datos de firma del terminal y encapsula los datos de firma del terminal y la clave pública en un formato especificado, y envía los datos de formato especificado al cliente
S106
El cliente envía los datos de formato especificado al servidor, de modo que el servidor envía la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión del cliente y la información de uso del certificado a una CA después de determinar, de acuerdo con la clave pública, que los datos de firma del terminal y el identificador de aplicación están verificados
S108

FIG. 1

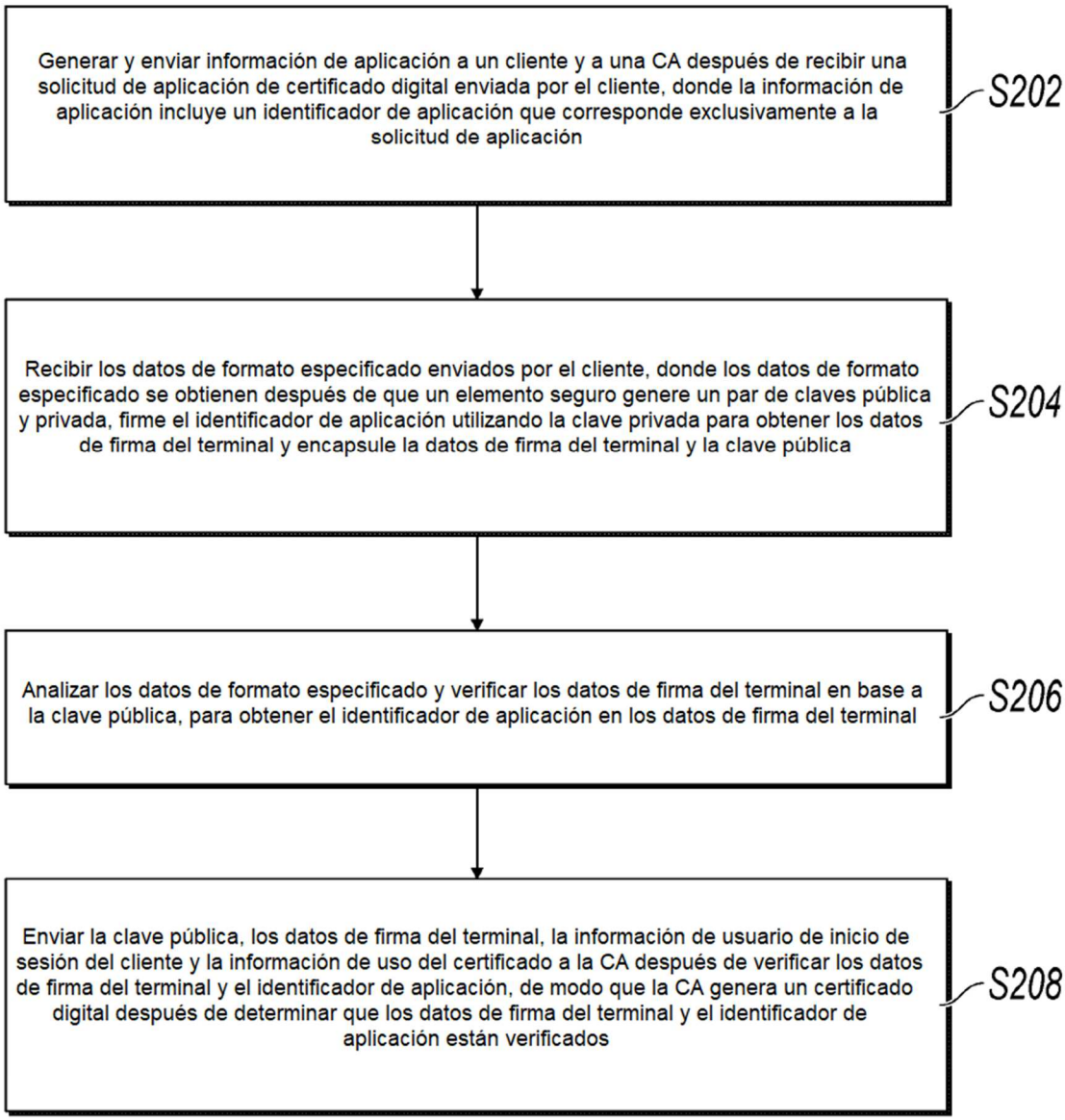
Generar y enviar información de aplicación a un cliente y a una CA después de recibir una solicitud de aplicación de certificado digital enviada por el cliente, donde la información de aplicación incluye un identificador de aplicación que corresponde exclusivamente a la solicitud de aplicación
S202
Recibir los datos de formato especificado enviados por el cliente, donde los datos de formato especificado se obtienen después de que un elemento seguro genere un par de claves pública y privada, firme el identificador de aplicación utilizando la clave privada para obtener los datos de firma del terminal y encapsule la datos de firma del terminal y la clave pública
S204
Analizar los datos de formato especificado y verificar los datos de firma del terminal en base a la clave pública, para obtener el identificador de aplicación en los datos de firma del terminal
S206
Enviar la clave pública, los datos de firma del terminal, la información de usuario de inicio de sesión del cliente y la información de uso del certificado a la CA después de verificar los datos de firma del terminal y el identificador de aplicación, de modo que la CA genera un certificado digital después de determinar que los datos de firma del terminal y el identificador de aplicación están verificados
S208

FIG. 2

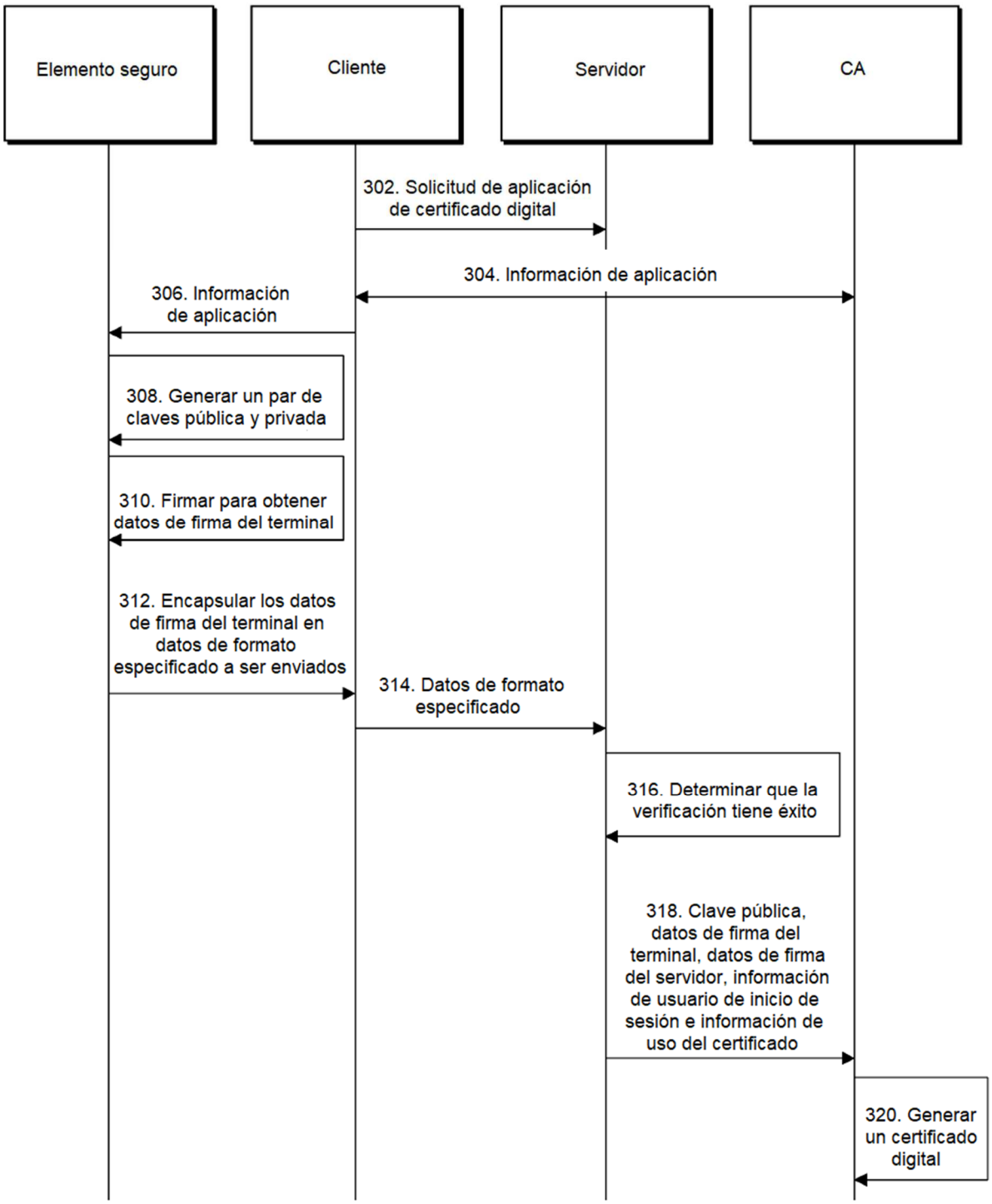
Elemento seguro
Cliente
Servidor
CA
302. Solicitud de aplicación de certificado digital
304. Información de aplicación
306. Información de aplicación
308. Generar un par de claves pública y privada
310. Firmar para obtener datos de firma del terminal
312. Encapsular los datos de firma del terminal en datos de formato especificado a ser enviados
314. Datos de formato especificado
316. Determinar que la verificación tiene éxito
318. Clave pública, datos de firma del terminal, datos de firma del servidor, información de usuario de inicio de sesión e información de uso del certificado
320. Generar un certificado digital

FIG. 3

Tipo	Etiqueta(T)	Longitud(L)	Valor(V)	Etiqueta(T)	Longitud(L)	Valor(V)	Etiqueta(T)	Longitud(L)	Valor(V)
RSA	6E	00 (256 bytes)	Longitud de clave	65	04	00010001	80	00 (256 bytes)	Datos de firma

FIG. 4

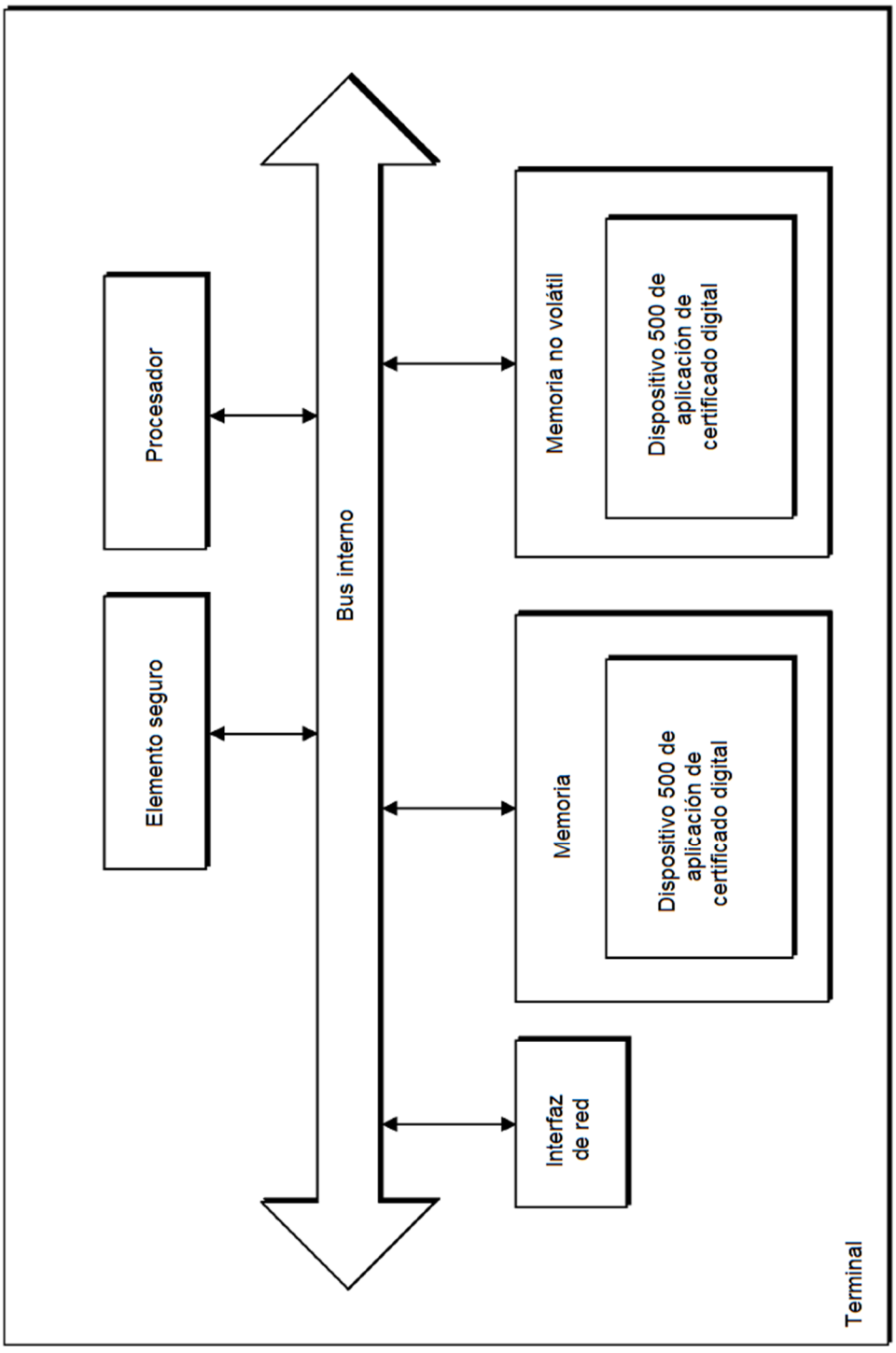
Terminal
Procesador
Elemento seguro
Bus interno
Interfaz de red
Memoria
Dispositivo 500 de aplicación de certificado digital
Memoria no volátil
Dispositivo 500 de aplicación de certificado digital

FIG. 5

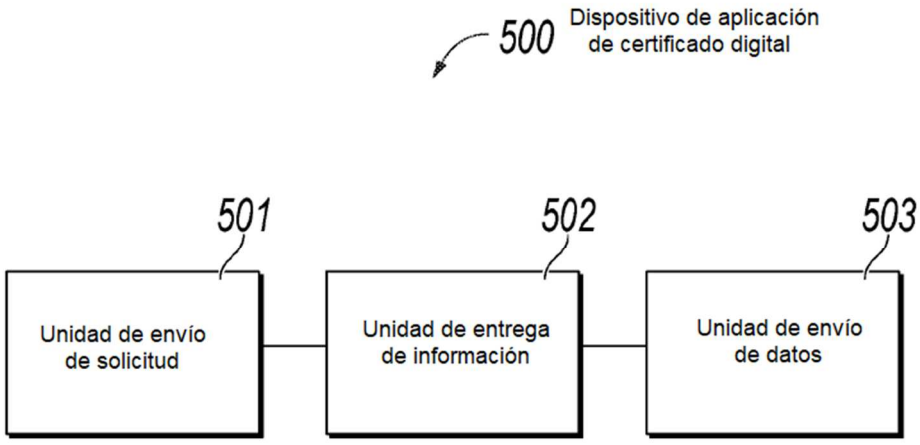
500
Dispositivo de aplicación de certificado digital
501
502
503
Unidad de envío de solicitud
Unidad de entrega de información
Unidad de envío de datos

FIG. 6

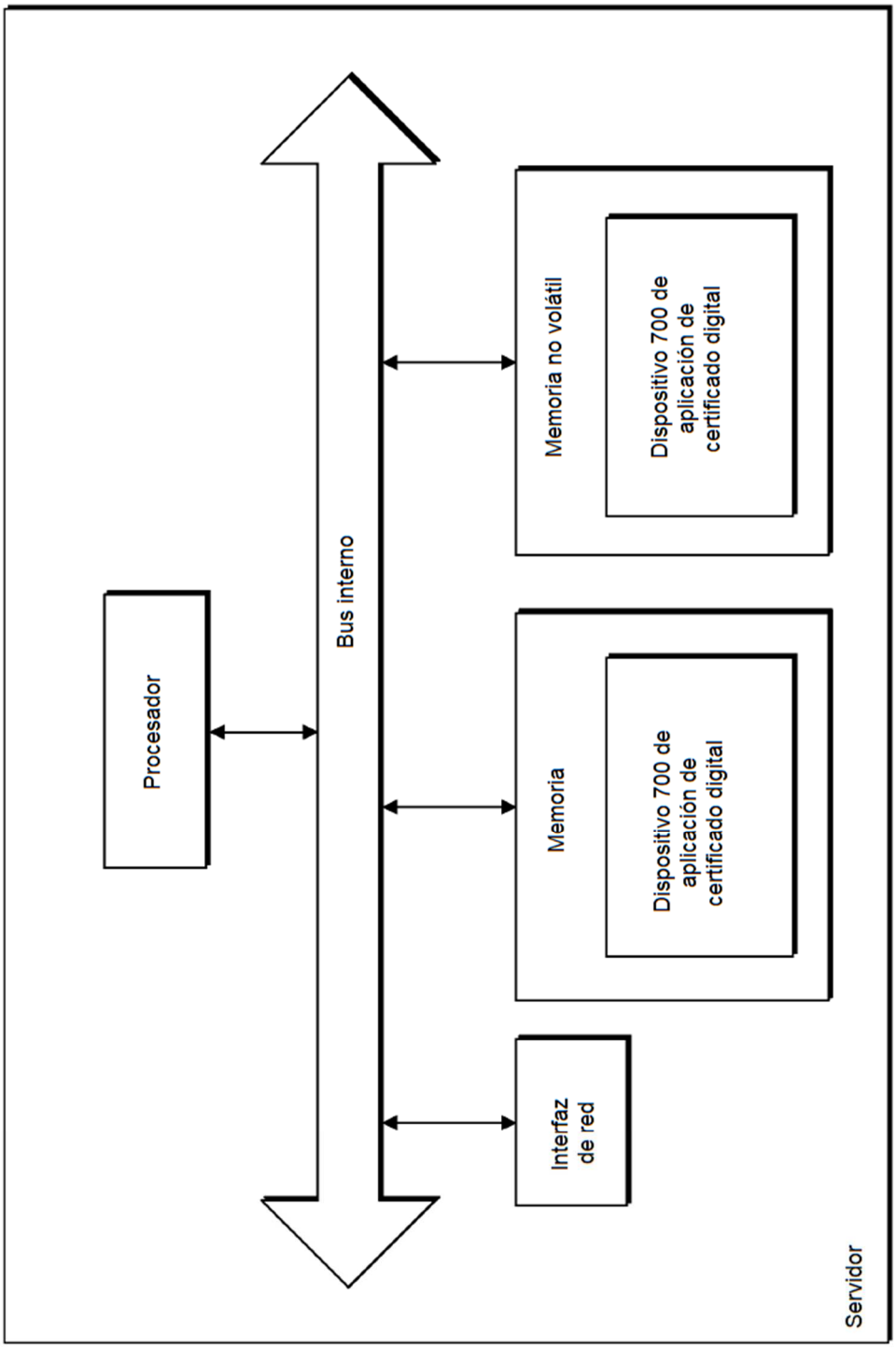
Procesador
Bus interno
Memoria no volátil
Dispositivo 700 de aplicación de certificado digital
Memoria
Dispositivo 700 de aplicación de certificado digital
Interfaz de red
Servidor

FIG. 7

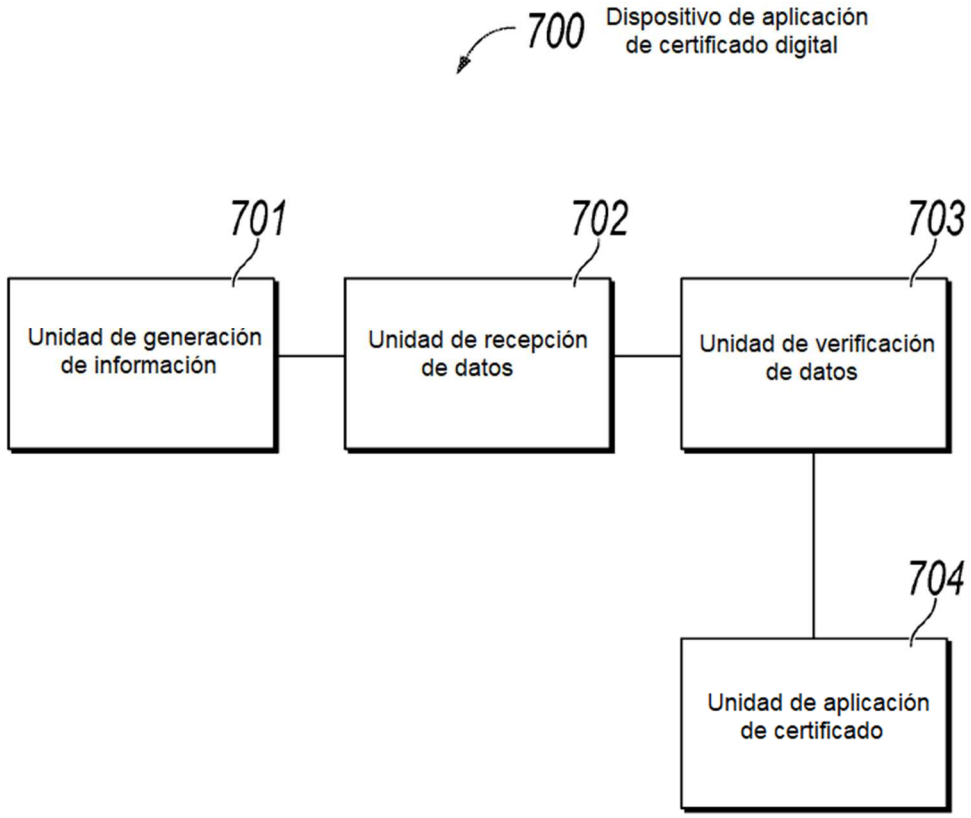
700
Dispositivo de aplicación de certificado digital
701
Unidad de generación de información
702
Unidad de recepción de datos
703
Unidad de verificación de datos
704
Unidad de aplicación de certificado

FIG. 8

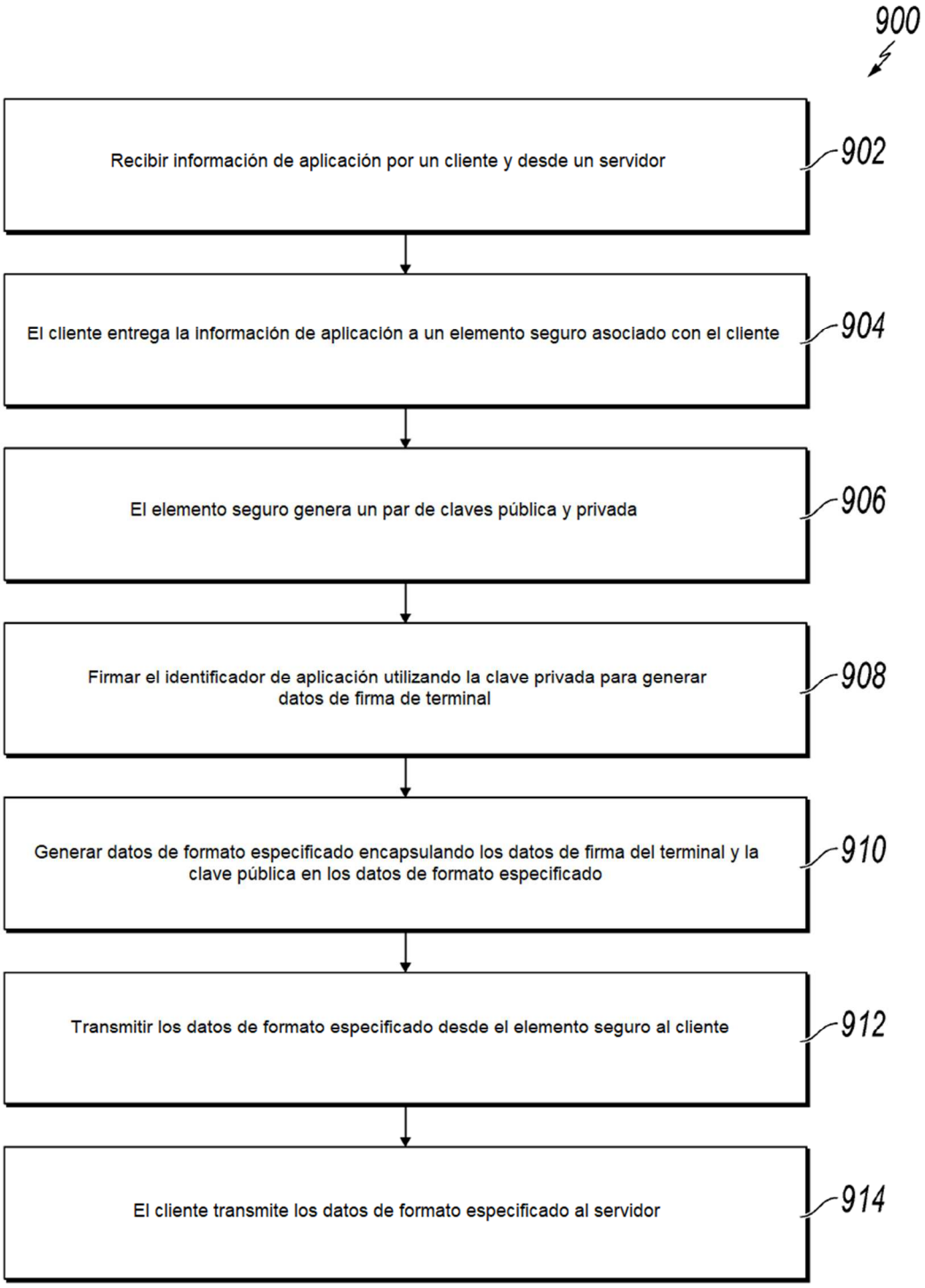
900
Recibir información de aplicación por un cliente y desde un servidor
902
El cliente entrega la información de aplicación a un elemento seguro asociado con el cliente
904
El elemento seguro genera un par de claves pública y privada
906
Firmar el identificador de aplicación utilizando la clave privada para generar datos de firma de terminal
908
Generar datos de formato especificado encapsulando los datos de firma del terminal y la clave pública en los datos de formato especificado
910
Transmitir los datos de formato especificado desde el elemento seguro al cliente
912
El cliente transmite los datos de formato especificado al servidor
914

FIG. 9