(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 695 245**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
G06F 21/64 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **04.12.2013 E 13382493 (8)**

(97) Fecha y número de publicación de la concesión europea: **19.09.2018 EP 2882156**

(54) Título: **Método implementado por ordenador y un sistema informático para evitar problemas de seguridad en el uso de certificados digitales en la firma de códigos y un producto de programa informático de los mismos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.01.2019

(73) Titular/es:

TELEFÓNICA DIGITAL ESPAÑA, S.L.U. (100.0%)
Gran Via 28
28013 Madrid, ES

(72) Inventor/es:

DE LOS SANTOS, SERGIO;
BARROSO BERRUETA, DAVID;
GUZMÁN SACRISTÁN, ANTONIO;
DE LA ROSA, TERO y
ALONSO CEBRIÁN, JOSÉ MARÍA

(74) Agente/Representante:

ARIZTI ACHA, Monica

DESCRIPCIÓN

Método implementado por ordenador y un sistema informático para evitar problemas de seguridad en el uso de certificados digitales en la firma de códigos y un producto de programa informático de los mismos

Campo de la técnica

La presente invención se dirige, en general, al campo de la seguridad informática. En particular, la presente invención divulga un método implementado por ordenador y un sistema informático para evitar problemas de seguridad en el uso de certificados digitales en la firma de códigos y un producto de programa informático de los mismos.

Antecedentes de la invención

El uso de firmas digitales para certificar la autoría de un archivo de software es un procedimiento ampliamente adoptado por las empresas líderes en el desarrollo y la distribución de software. La adopción de firmas digitales comporta la integración de una compleja infraestructura en los entornos de desarrollo de código y los sistemas operativos en los que se ejecutará este código. Ciertamente, el uso de software firmado evita múltiples amenazas definidas para la generación y la distribución de software; no obstante, debido a que este también comporta la incorporación de nuevos componentes y servicios, es posible identificar nuevas amenazas que podrían afectar al propio proceso de firma.

El elemento clave de esta infraestructura es el uso de la criptografía de clave pública. Esto posibilita que los diseñadores mantengan los procesos de firma y los procesos de verificación de firma de manera independiente, sin la necesidad de un intercambio anterior de claves secretas. La independencia de estos dos procesos facilita el establecimiento de una clasificación para categorizar las amenazas de acuerdo con el proceso para el que estas están definidas. El robo de certificados (con la puesta en peligro o la exposición no controlada de la clave privada asociada), el uso inapropiado de certificados, directivas poco adecuadas para la actualización de certificados y los problemas en la cadena de certificación (rotura o modificación) son las fuentes de varias amenazas que afectan a ambos procesos, a pesar de que los objetivos que se persiguen son diferentes si ha sido atacado el proceso de firma o el proceso de verificación.

La criptografía responde de manera eficiente a la necesidad de identificación de extremos en cualquier proceso de comunicación. Se han definido diferentes mecanismos criptográficos para lograr esta tarea, pero el más extendido es el uso de certificados digitales. Estos se construyen sobre la base de la criptografía de clave pública. La tarea de identificar los extremos se asume por autoridades de certificación (CA), las cuales se identifican, a su vez, por tales extremos, como entidades de confianza. Es necesario que quien se encuentre tras la clave pública contenida en un certificado dado haya sido identificado de manera apropiada por las autoridades de emisión de certificados. También es preciso que una autoridad de certificación particular pueda identificarse usando su propia clave pública. Una identificación correcta puede lograrse solo si estos dos requisitos se ven satisfechos.

A pesar de que los certificados digitales son fundamentales en la identificación de sitios web, estos son también los elementos clave en los procesos de firma. La gestión de certificados ha de ser coherente con una Infraestructura de Clave pública adecuada para proporcionar protocolos para implementar los procesos en relación con la firma de archivos (firma de códigos). Un par de claves, una pública y una privada, se genera para cada usuario o entidad para el cifrado y el descifrado. Tal como se ha indicado anteriormente, para asegurar la confiabilidad de las claves públicas/privadas, las autoridades de certificación (CA) emiten certificados de clave digital. Estos certificados se firman de manera digital por las CA para garantizar que un individuo que proporciona un certificado digital es quien el individuo reivindica ser. Mediante la emisión del certificado, una CA está aseverando que el contenido del certificado es de aplicación al sujeto certificado. Cuando el sujeto de certificado presenta el certificado a los usuarios de confianza, los usuarios de confianza pueden usar certificados digitales para autenticar el sujeto de certificado. Esta certificación es válida hasta la fecha de caducidad especificada por la CA. Si el certificado no ha caducado, el proceso de autenticación habitualmente comporta dos fases: el primer lugar, la validación de integridad del certificado usando la clave pública de la CA, y en segundo lugar, verifica que el sujeto del certificado tiene acceso a una clave privada asociada con el certificado del sujeto.

En ocasiones, puede ser necesario que los certificados digitales se revoquen antes de la caducidad, por ejemplo cuando la privacidad de la contraseña privada del sujeto se ha visto comprometida. El certificado revocado se publica entonces en una base de datos de información de estado de certificado administrada por CA, tal como la lista de revocación de certificados (CRL). Cuando un usuario de confianza usa el certificado para autenticar un sujeto de certificado, el usuario de confianza puede determinar el estado de revocación del certificado mediante el acceso directo a esta base de datos de información de estado de certificado. No obstante, la arquitectura de CA es una solución puramente centralizada. Con frecuencia, tienen lugar latencias elevadas y problemas de disponibilidad. Con el fin de eliminar la necesidad de conectividad con la PKI cuando es preciso que el usuario de confianza

autentique la identidad del sujeto de certificado, un enfoque prevé que cada sujeto de certificado adquiera periódicamente su estado a partir de CRL o que obtenga un estado de OCSP para su sujeto de certificado de un servidor de OCSP. Estas soluciones heredan los problemas de disponibilidad que se han mencionado anteriormente, provocando problemas con la actualización de información de revocación [1]. En 2012, Google Inc. propuso migrar la información contenida en la CRL al navegador [2]. Esto significa abandonar el esquema centralizado tradicional por un esquema distribuido, eliminando el cuello de botella que están siendo los servidores de OCSP, o el servidor de CRL, anteriores.

En realidad, la firma de códigos es una aplicación importante particular de estos certificados digitales. El proceso de firma de códigos consiste en firmar de manera digital archivos ejecutables y otros archivos que pueden interpretarse por una plataforma de tiempo de ejecución para asegurar que estos archivos no se han alterado. Ahora es posible identificar un código como proveniente de una fuente específica y determinar si el código es de confianza para un fin específico (Figura 1). Hay dos métodos principales para la firma de códigos: los desarrolladores/distribuidores puede elegir proporcionar su propio par autogenerado de claves (privada/pública) y estos tienen que proporcionar la clave pública al usuario de algún modo, tal como se divulga en la patente US 7.370.206; o debería poderse rastrear la clave pública usada para autenticar la firma de código de vuelta a una autoridad CA raíz de confianza usando una PKI segura. Además, el segundo método tampoco asegura que pueda confiarse en el código; este método solo asegura que el código se firmó por el sujeto del certificado. Una CA proporciona un nivel de confianza raíz y es capaz de asignar confianza a otros mediante apoderado. Si un usuario confía en una CA, entonces el usuario puede confiar, presumiblemente, en la legitimidad del código que se firma con una clave generada por esa CA o uno de sus apoderados. Muchos sistemas operativos y marcos de trabajo contienen una confianza incorporada para una o más CA existentes. Habitualmente, una firma de código consiste en tres partes:

- Un resumen de archivo, que es una colección de sumas de comprobación o funciones de troceo de las diversas partes del código. El resumen puede usarse para detectar alteraciones en el código y en el identificador de aplicación.
- Una firma digital, que se realiza por el usuario legítimo con su clave privada y se usa para firmar el resumen para garantizar su integridad. Por lo tanto, la firma incluye una información que puede usarse para determinar quién firmó el código y si la firma es válida.
- Un identificador único, el cual puede usarse para identificar el código o para determinar a qué grupos o categorías pertenece el código.

Como cualquier medida de seguridad, la firma de códigos puede neutralizarse. Puede engañarse a los usuarios para que ejecuten un código no firmado, o incluso para que ejecuten un código que se niega a validarse. También es importante observar que la firma de códigos no protege al usuario final frente a cualquier actividad maliciosa o errores de software no intencionados realizados por el autor del software [3]. Desafortunadamente, ni siquiera el uso correcto de firmas de software puede proteger a los usuarios finales. Si no se puede asegurar que no hay infracción de seguridad alguna en la totalidad del proceso de firma, ha de suponerse que el software resultante puede haberse visto comprometido. Esto significa, entre otras infracciones de seguridad, que puede haberse violado la integridad de los certificados digitales y la integridad de archivo firmado.

Los objetivos deseados por un atacante de un sistema de software de firma son:

- Engañar al firmante para que firme un archivo diferente del previsto o bajo unas condiciones no previstas cambiando las reglas o directivas establecidas en los requisitos de firma.

- Acceso no autorizado a los datos de creación de firma.

- Sustituir la información firmada. El atacante intenta sustituir parte o la totalidad de la información firmada por su propio beneficio cuando la firma de archivo se ha calculado.

- Hacer que el archivo firmado se atribuya a un usuario diferente del verdadero firmante. El atacante pretende que un archivo firmado por un determinado firmante se verifique como firmado por una entidad diferente. De ese modo, el atacante podría provocar la atribución de autoría de un archivo erróneo.

- Hacer que el archivo firmado se atribuya a un usuario diferente del usuario legítimo. El atacante pretende que un archivo firmado por el firmante legítimo se verifique como firmado por una entidad diferente. De esta forma, el atacante podría provocar la atribución incorrecta de la autoría de un archivo.

- Hacer que el archivo se verifique contenga una información elegida. El atacante pretende que el archivo firmado se muestre al verificador también con un contenido cuya apariencia pueda ser diferente de lo que se firmó en realidad.

- Hacer que la verificación de firma concluya con un resultado opuesto. La integridad de la firma depende no solo

de la propia firma sino también de la validez del certificado.

Para alcanzar estos objetivos, pueden documentarse múltiples técnicas de ataque. Una clasificación completa para estos se muestra en la tabla 1, formulada en siete categorías diferentes [4]:

Tabla 1: Amenazas definidas para el proceso de firma y los procesos de verificación de firma.

Manipulación del entorno de ejecución de ambos procesos.	Modificación de Documento	Inclusión de contenido dinámico	Código oculto
			Código activo
			Código enlazado
		Modificación de contenidos	
	Modificación de Atributos	Inclusión de contenido dinámico	Código oculto
			Código activo
			Contenido enlazado
		Modificación de contenidos	
	Modificación de datos a firmar		
	Modificación de representación de datos a firmar		
Modificación antes del cálculo de la firma.	Contenido externo		
	Criptoanálisis	Función de troceo	Ataque de colisión
			Ataque de preimagen
			Ataque de segunda preimagen
Modificación antes del cálculo de la firma.	Puesta en peligro de los datos de autenticación del firmante	Ingeniería social	
		Interceptación de datos de autenticación del firmante	Observación
			Interceptación en comunicación interproceso/entidades
			Puesta en peligro de puntos de extremo
		Adivinación	
	Omisión de autenticación		
Puesta en peligro de los datos usados en el cálculo de la firma.	Interceptación de Datos de creación de firma	Interceptación en comunicación interproceso/entidades	
		Puesta en peligro de puntos de extremo	
	Escucha furtiva (canal paralelo)	Análisis de sincronismo	
		Análisis electromagnético	
		Análisis de potencia	
		Análisis de microarquitectura	
		Observación óptica	
	Acceso no autorizado a los dispositivos de creación de firma	Puesta en peligro de los datos de autenticación del firmante	
		Omisión de Autenticación	
	Criptoanálisis	Algoritmo asimétrico	
	Ataques de manipulación indebida invasiva		
Manipulación indebida del resultado de la verificación de certificados.	Alteración de la solicitud de revocación del abonado		
	Alteración de la verificación de estado de certificado	Omisión de periodo de gracia o de precaución	Retardo en el envío de firma con sello de tiempo
			Retardo en el envío de firma con marca de tiempo
			Aprovechar retardo en el procesamiento de solicitud de revocación de la CA
		Modificación de solicitud de la verificación de estado de certificado	Modificación de solicitud de OCSP
			Modificación de solicitud basada en LDAP

		Modificación de la respuesta de la verificación de estado de certificado	
		Alteración de la verificación de referencia de tiempo	Modificación de sello de tiempo
			Modificación de marca de tiempo
		Contestación de información de validación	Contestación de respuesta de OCSP
		Alteración del resultado de verificación de estado de certificado	
	Ancla de confianza en el que no se confía		
	Alteración del resultado de verificación de integridad de certificado		
	Alteración de resultado de verificación de periodo de validez del certificado		
Manipulación indebida del resultado de la verificación de firma.	Manipulación de la presentación	Enmascaramiento de los datos a verificar	Enmascaramiento de Documento
			Enmascaramiento de Atributos
		Manipulación del visualizador	Sustitución de visualizador
			Alteración del comportamiento del visualizador
		Enmascaramiento de resultado de verificación	
	Sustitución de Directivas	Sustitución de directivas de firma electrónica	
		Sustitución de directivas de certificado	
	Alteración del proceso de verificación	Inyección de par de datos firmado con firma	
		Alteración de resultado de verificación criptográfica	
		Alteración de resultado de verificación final	

Provocar una manipulación del entorno o lograr una modificación antes del cálculo de la firma un atacante puede engañar al firmante para que firme un documento diferente del previsto o bajo unas condiciones no previstas. La realización de una invocación no autorizada de la función de firma o la puesta en peligro de los datos de creación de firma puede suponer un uso autorizado de datos de creación de firma. Una modificación después del cálculo de la firma provocará una sustitución de información firmada. La manipulación indebida del resultado de verificación de certificado o el resultado de verificación de firma puede atribuir al documento firmado autoridad para un usuario diferente del firmante legítimo. Por otro lado, una manipulación del entorno, junto con una influencia sobre el resultado de verificación de firma, puede hacer que los datos a verificar se muestren con un contenido modificado de manera maliciosa. Por último, la manipulación indebida del resultado de verificación de certificado y/o la manipulación indebida del resultado de verificación de firma pueden hacer que la verificación de validez de firma concluya con un resultado opuesto.

En la Tabla 1 se ha mostrado que, dejando de lado la manipulación del entorno de ejecución de los procesos de firma y de verificación, la totalidad de las categorías contienen amenazas en relación con los problemas de seguridad derivados del uso indebido de los certificados digitales. La totalidad de estas amenazas se marcan en la tabla 1 y puede suponer la implementación de diferentes tipos de ataques: emisión inapropiada provocada por un análisis sintáctico de CA incorrecto; análisis sintáctico de navegador incorrecto de los certificados digitales; ataques de intermediario; ataques de revinculación; abuso de la información de ancla de confianza en las trayectorias de validación de certificación; robo de certificado digital, etc.

Algunas de las soluciones existentes para varios de estos ataques se han descrito anteriormente, pero hay otras soluciones que necesitan un análisis más profundo. En 2007, la industria de las autoridades de certificación desarrolló una tecnología denominada certificados de validación extendida (EVC) con el fin de mejorar la seguridad en la emisión de certificados. A diferencia de los certificados normales, los cuales indican solo que el propietario controla un nombre de dominio particular, los certificados de validación extendida también confirman la identidad de una empresa legítima. Se precisa una mención especial para las soluciones que se proporcionan para resolver el abuso de la información de ancla de confianza y los ataques de intermediario usando una técnica denominada fijación de certificado. EMET es una herramienta desarrollada por Microsoft como un conjunto de software de protección que contiene soluciones para diferentes problemas de seguridad. Una de estas soluciones proporciona una técnica que propone unirse a dominios de Internet con certificados emitidos por autoridades de certificación raíz presentes en el almacén de certificados de confianza del usuario. Otra opción se proporciona por Google, que propone modificar el navegador web (es decir, Chrome). Chrome ha añadido a su código fuente algunos sitios web que siempre funcionarán con HTTPS activo desde el principio. Estos sitios web se denominan “sitios HTST precargados”. Además de requerir el uso del protocolo SSL desde el inicio de la conexión, el navegador de Google recordará qué claves públicas se conocen y rechazará el resto, incluso si el usuario no escribe https en la barra de direcciones del navegador. Los datos de las autoridades en esta fijación de certificado para verificar la firma de archivos de software. Por otro lado, el uso de certificados de validación extendida puede verse comprometido por ataques de revinculación. Ni los certificados de validación extendida ni las soluciones de fijación de certificado pueden hacer nada para evitar el robo de los mismos.

Los certificados digitales presentes en los archivos binarios de un producto de software están diseñados para garantizar la integridad y la autenticidad de estos archivos. Existen varias razones para probar por qué puede ser necesario que un atacante use certificados adquiridos ilegitimados para firmar su propio código.

- Las soluciones de antivirus otorgan habitualmente un nivel de confianza más alto a los archivos firmados por autoridades de confianza.
- El usuario final (o la víctima) confía en los archivos firmados debido a la firma, con independencia del origen del certificado usado. También es un factor contributivo el hecho de que los programas de verificación como Microsoft Authenticode codifican con colores la confiabilidad de un archivo: el color verde se corresponde con un archivo de confianza y firmado.
- En los sistemas operativos modernos, se requiere una firma digital correcta para realizar algunas tareas, como la instalación del controlador de dispositivo. Si un atacante desea penetrar en el sistema de una manera silenciosa, es preciso que este firme su paquete raíz con un certificado válido.

En la actualidad, cuando se detecta un certificado sustraído, el propietario solicita su revocación. Esta revocación comporta publicar este en una lista negra pero este proceso presenta varios inconvenientes:

- Cuando se detecta el robo del certificado, es imposible saber durante cuánto tiempo ha estado este certificado en posesión del atacante.
- En el caso de un software de firma, la revocación de certificado no es siempre posible debido a que los archivos binarios firmados podrían no funcionar de manera apropiada.
- Existen problemas en relación con retardos en la actualización de información a partir de las listas negras de OCSP y CRL.

Así, no hay solución alguna para defender a un usuario final de archivos de software o archivos binarios firmados frente al abuso de certificados digitales o la puesta en peligro de las cadenas de confianza asociadas con los mismos. Por lo tanto, la presente invención proporciona una solución para mitigar el efecto del robo de certificados y autoridades de certificación comprometidas. La invención permite que el usuario verifique la integridad de un archivo dado.

El documento WO 01/41360 A2 proporciona métodos para manejar objetos originales electrónicos almacenados que se han creado firmado objetos de información por respectivos agentes de tratamiento, enviando objetos de información firmada a una utilidad de custodia de confianza, validando los objetos de información firmados enviados probando al menos la integridad de los contenidos de cada objeto de información firmado y la validez de la firma del respectivo agente de transferencia y aplicando a cada objeto de información validado una indicación de tiempo y fecha y una firma digital y certificado de autenticación de la utilidad de custodia de confianza.

El documento US5638446 divulga un proceso para usar una tercera parte de confianza para crear un certificado electrónico para un archivo electrónico que puede usarse para establecer el archivo y verificar la identidad del creador del archivo. El proceso se compone de dos fases, una fase de registro y una fase de distribución de archivo electrónico. En la fase de registro, una tercera parte de confianza recibe información acerca de un autor, que incluye la clave pública del autor y verifica afirmativamente la precisión de esta información. En la fase de distribución de archivo, un autor envía a la tercera parte de confianza un mensaje que contiene la función de troceo del archivo que

el autor quiere distribuir. La tercera parte de confianza crea un certificado electrónico, firmado por tercera parte de confianza, que contiene la función de troceo del archivo enviado por el autor. Un usuario que desea recibir los archivos recupera el archivo con el certificado y usa el certificado para verificar, primero, que la tercera parte de confianza creó el certificado, y, segundo, que la función de troceo del archivo en el certificado es la misma que la función de troceo que se calcula a partir del archivo recuperado. Si estas dos funciones de troceo coinciden, entonces el usuario se asegura que el archivo sí se originó con el autor y está incorrupto.

El documento WO 2004/004855 A1 divulga un método para terminales de juego, quioscos de juego y terminales de lotería para asegurar que puede confiarse en el proceso de verificación de firma de código de software de juego descargado. Controladores desarrollados independientemente del suministrador del sistema operativo están embebidos dentro del núcleo del sistema operativo para verificar que los componentes de hardware microcodificados, el BIOS (808), los componentes de sistema operativo y el software de juego descargado pueden confiarse.

Referencias

[1] CLARK, Jeremy; VAN OORSCHOT, Paul C. SoK: SSL y HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. 2012.
[2] TOPALOVIC, Emin, y col. Towards Short-Lived Certificates. Web 2.0 Security and Privacy, 2012.
[3] SENESE, Thomas J.; KRUEGEL, Chris A.; WOODWARD, Timothy G. METHOD y APPARATUS FOR AUTHENTICATING A DIGITAL CERTIFICATE STATUS AND AUTHORIZATION CREDENTIALS. Patente de Estados Unidos Nº. 20.130.072.155, 21 de Marzo de 2013.
[4] HERNÁNDEZ-ARDIETA, Jorge López. Enhancing the reliability of digital signatures as non-repudiation evidence under a holistic threat model. 2011. Tesis Doctoral. Universidad Carlos III de Madrid.

Descripción de la invención

La invención se define en las reivindicaciones independientes.

Para conseguir lo anterior, la presente invención proporciona una infraestructura en la que un distribuidor de software que ha firmado uno o más archivos de software (archivos ejecutables binarios, etc.) puede grabar todos los datos en relación con esta firma digital. Esto determinará cómo se realizó la firma de certificado, qué archivo de software se firmó, en qué momento se publica esta información y cómo era la cadena de certificados de confianza en el momento de la publicación. De esta forma, cualquier usuario que haya adquirido una copia del archivo de software firmado y haya validado que la firma digital se corresponde con un certificado digital válido, puede verificar ahora si existe algún problema en relación con el uso indebido del certificado digital.

Además, se propone un procedimiento para permitir que el usuario final que ha adquirido una copia de un archivo de software firmado contraste los datos contenidos en la firma de archivo de software con los datos almacenados en la infraestructura propuesta por el distribuidor de software y comprobar si ha existido algún cambio en la cadena de certificados de confianza.

Por lo tanto, de acuerdo con un primer aspecto de la presente invención, se proporciona un método implementado por ordenador para evitar problemas de seguridad en el uso de certificados digitales en la firma de códigos, que comprende como comúnmente en el campo: firmar, por un distribuidor de software a través de un primer servidor, por lo menos un archivo de software usando un certificado digital con una firma digital que identifica a dicho distribuidor de software; y adquirir, por al menos un usuario a través de un dispositivo de cálculo, una copia de dicho por lo menos un archivo de software firmado.

De una manera característica y en contraposición a las propuestas conocidas, el certificado digital que va a usarse para la firma del archivo de software se graba con anterioridad en un segundo servidor en comunicación con dicho primer servidor, estando proporcionado el certificado digital que va a grabarse por el distribuidor de software tras un registro de este último en dicho segundo servidor e incluyendo el certificado digital una información que se obtiene a partir de una cadena de certificados de confianza asociada con el certificado digital cuando se realiza dicho registro. Además, el segundo servidor también genera, tras una solicitud realizada por el distribuidor de software, una indicación de función de troceo del por lo menos un archivo de software firmado.

El registro comprende comprobar, por el segundo servidor, datos incluidos en el certificado digital proporcionado que incluyen por lo menos un dominio y/o una dirección electrónica. Además, el método también puede lograr varias verificaciones con el fin de certificar la relación de un nuevo certificado con una cuenta de distribuidor de software existente. Por ejemplo, puede realizarse una segunda autenticación del certificado digital por el segundo servidor por medio de: generar una contraseña de un solo uso (OTP); enviar, dicha contraseña de un solo uso (OTP) generada al distribuidor de software a través de un canal de comunicación que incluye por lo menos un mensaje de texto, un mensaje electrónico o un mensaje instantáneo; y certificar, tras la recepción de dicha OTP a partir del distribuidor de

software, que la OTP que se recibe coincide con dicha OTP generada.

Incluso, antes de que se grabe un nuevo certificado, el segundo servidor puede comprobar el estado de revocación y de caducidad del certificado digital proporcionado y la validez de la cadena de certificados de confianza. Así, en el caso de que haya cualquier anomalía un sistema de alerta en el segundo servidor puede informar al distribuidor de software. Específicamente, una vez que se ha obtenido la cadena de certificados de confianza para el certificado digital particular, la relación entre la totalidad de las autoridades de certificación intermedias se analiza por medio de búsqueda de irregularidades.

De acuerdo con una primera alternativa, el distribuidor de software puede usar, con el fin de solicitar la generación de dicha indicación de función de troceo, un programa especializado para extraer la firma digital del archivo de software firmado y enviar esta al segundo servidor junto con el nombre del archivo de software firmado.

De acuerdo con una segunda alternativa, para solicitar la generación de la indicación de función de troceo, el distribuidor de software puede cargar el archivo de software firmado directamente al segundo servidor. En esta segunda alternativa, la extracción de información de la firma digital del archivo de software y la siguiente verificación se realiza por el segundo servidor.

La indicación de función de troceo generada incluye una información acerca del distribuidor de software y acerca del archivo de software firmado y un registro de tiempo que certifica un momento en el que la firma del archivo de software se notifica al distribuidor de software.

De acuerdo con una realización, el segundo servidor puede aprovechar la información que se proporciona por fuentes remotas tal como una autoridad de certificación (CA) o un protocolo de estado de certificado en línea (OCSP) para comprobar el estado del certificado o los certificados que se proporcionan. Este también ejecuta un motor de metabúsqueda o rastreador web para buscar diferentes instancias del archivo de software firmado en la web. Cuando se encuentra una de estas instancias, se ejecuta un procedimiento de verificación de firma sobre este archivo. Si hay cualquier anomalía en relación con el certificado digital, el segundo servidor genera una alerta para informar al distribuidor de software de que existe un problema potencial en relación con el certificado digital. El segundo servidor forzaría la revocación del certificado digital sospechoso en el caso de ser un certificado digital comprometido.

En este caso, una vez que el estado del certificado digital ha cambiado y ha acabado por revocarse, el segundo servidor cambia de manera inmediata el estado del archivo de software firmado y notifica a dicho por lo menos un usuario, que el archivo de software firmado adquirido no es de confianza. En cualquier caso, si el distribuidor de software decide que un certificado se ha visto comprometido, este puede ir al segundo servidor y revocar directamente el certificado digital.

Así, una vez que se ha generado la indicación de función de troceo de un archivo de software firmado, dicho usuario, como una característica de la presente invención, puede verificar si su copia adquirida coincide con el archivo de software firmado al que se ha aplicado indicación de función de troceo registrado con el segundo servidor. Para hacer esto, el usuario comprobará la validez de la firma digital de la copia adquirida del archivo de software firmado y extraerá, usando un programa especializado, datos de firma a partir de la copia adquirida del archivo de software firmado. Entonces, el usuario solicitará una validación de indicación de función de troceo al segundo servidor. Cuando el segundo servidor recibe esta solicitud, puede comprobar si este certificado digital se ha grabado en el sistema, recuperar un resumen al que se ha aplicado función de troceo y usar este resumen por aplicación de función de troceo como un índice. A continuación, puede devolver la totalidad de la información almacenada durante la creación de la indicación de función de troceo. Esta información permitirá que el segundo servidor verifique la cadena de certificados de confianza y determine el estado de certificado en comparación con el certificado almacenado durante el registro de certificado digital.

Lo que es más, el usuario puede verificar si el distribuidor de software esperado fue en realidad el que firmó el archivo de software y cuándo firmó este el archivo de software. En este caso, las comprobaciones habituales con el fin de validar la firma digital se realizan por el segundo servidor, el cual extraerá datos de firma a partir de la copia adquirida del archivo de software firmado y comprobará que se corresponde con el distribuidor de software. Entonces, el segundo servidor recuperará un resumen al que se ha aplicado función de troceo y usará este como un índice para buscar información de indicación de función de troceo con respecto a la copia adquirida. Esta información permitirá que el segundo servidor verifique la cadena de certificados de confianza y determine el estado de certificado en comparación con el certificado almacenado durante el registro de certificado.

Complementario de dicha revocación de certificado digital, el método también prevé un procedimiento para detecta una relación no permitida entre certificados digitales y funciones de troceo de archivo de software. Este procedimiento se ejecuta por el segundo servidor, el cual intercepta la totalidad de las solicitudes que se realizan por los usuarios que adquirieron una copia del archivo de software firmado. En el caso de que una solicitud consulte

acerca de un archivo de software firmado correctamente con un certificado digital, y el certificado digital se grabe por el segundo servidor pero no exista la asociación certificado-función de troceo de archivo correspondiente, el segundo servidor emite una advertencia al distribuidor de software y pone en cuarentena los otros archivos de software firmados usando ese certificado digital.

De acuerdo con un segundo aspecto, se proporciona un sistema informático para evitar problemas de seguridad en el uso de certificados digitales en la firma de códigos, que comprende: un primer servidor usado por un distribuidor de software que está configurado para firmar por lo menos un archivo de software usando un certificado digital con una firma digital de dicho distribuidor de software; y por lo menos un dispositivo de cálculo de usuario de un usuario para adquirir una copia de dicho por lo menos un archivo de software firmado. En contraposición a las propuestas conocidas, el sistema del segundo aspecto incluye además un segundo servidor en comunicación con dicho primer servidor que está configurado para grabar dicho certificado digital que va a usarse para dicha firma que incluye una información que se obtiene a partir de una cadena de certificados de confianza y que comprende unos medios para autenticar y registrar el distribuidor de software en su interior y unos medios para generar una indicación de función de troceo, tras una solicitud realizada por el distribuidor de software, del por lo menos un archivo de software firmado.

De acuerdo con una realización, comprendiendo además el sistema unos medios para usar una información que se proporciona a partir de fuentes remotas que incluyen por lo menos uno de una autoridad de certificación (CA) o un protocolo de estado de certificado en línea (OCSP) y/o unos medios para ejecutar un motor de metabúsqueda en una web.

La materia objeto que se describe en el presente documento puede implementarse en software en combinación con hardware y/o firmware, o una combinación adecuada de los mismos. Por ejemplo, la materia objeto que se describe en el presente documento puede implementarse en software ejecutado por un procesador.

De acuerdo con un tercer aspecto, se proporciona un producto de programa informático que comprende unos medios de código de programa informático que están adaptados para realizar las etapas de acuerdo con el método de la reivindicación 1 cuando dicho programa se ejecuta en un ordenador, un procesador de señales digitales, un campo de matrices de puertas programables, un circuito integrado específico de la aplicación, un microprocesador, un microcontrolador o cualquier otra forma de hardware programable.
El código de programa informático puede almacenarse en un medio legible por ordenador que pueda dirigir un ordenador, otro aparato programable de procesamiento de datos, u otros dispositivos que funcionen de una manera particular, de tal modo que las instrucciones almacenadas en el medio legible por ordenador produzcan un artículo de fabricación que incluya instrucciones que implementen la función/acción especificada en el bloque o bloques del diagrama de flujo y/o del diagrama de bloques.

Ha de apreciarse que se pretende que el término “procesador” tal como se usa en el presente documento incluya cualquier dispositivo de procesamiento, tal como, por ejemplo, uno que incluye una unidad de procesamiento central (CPU) y/u otra circuitería de procesamiento (por ejemplo, procesador de señales digitales (DSP), microprocesador, etc.). Adicionalmente, ha de entenderse que el término “procesador” puede hacer referencia a más de un dispositivo de procesamiento, y que diversos elementos asociados con un dispositivo de procesamiento pueden compartirse por otros dispositivos de procesamiento.

El sistema informático y el producto de programa informático implementan el método del primer aspecto.

Breve descripción de los dibujos

Las ventajas y características anteriores, y otras, se entenderán más completamente a partir de la siguiente descripción detallada de realizaciones, con referencia a lo adjunto, que ha de considerarse de una forma ilustrativa y no limitante, en lo que:

La Figura 1 ilustra el proceso de firma de archivos general.
La Figura 2 ilustra la arquitectura general de la presente invención.
La Figura 3 es un diagrama de flujo que ilustra cómo un nuevo certificado se graba en el segundo servidor de acuerdo con la presente invención.
La Figura 4 es un diagrama de flujo que ilustra cómo una indicación de función de troceo se genera de acuerdo con una primera alternativa de la presente invención.
La Figura 5 es un diagrama de flujo que ilustra cómo una indicación de función de troceo se genera de acuerdo con una segunda alternativa de la presente invención.
La Figura 6 es un diagrama de flujo que ilustra cómo un usuario puede verificar un estado de archivo de software firmado.
La Figura 7 es un diagrama de flujo que ilustra cómo un usuario puede verificar si el distribuidor de software esperado fue en realidad el que firmó el archivo de software y cuándo firmó este el archivo de software.

Descripción detallada de varias realizaciones

La presente invención proporciona una alternativa a la forma en la que se realiza tradicionalmente la verificación de los archivos firmados de manera digital publicados por un distribuidor de software 300 para los usuarios finales 100. Hoy en día, tal como puede verse en la Figura 2, un atacante 400 podría tener el control de un certificado digital emitido a un distribuidor de software 300 y este atacante 400 podría usar el certificado digital sustraído para firmar archivos de software como si este perteneciera a 300. El atacante 400 también podría comprometer a una autoridad de certificación intermedia de tal modo que es posible introducir una nueva autoridad de certificación intermedia que puede emitir certificados en el nombre del distribuidor de software 300. Por lo tanto, la presente invención propone el uso de un segundo servidor 200 que pueda mantener la información de los archivos firmados grabados/registrados por diferentes distribuidores de software.

Una vez que un distribuidor de software 300 se ha registrado en el segundo servidor 200 con el fin de hacer uso de sus servicios, es posible grabar los certificados digitales que van a usarse para firmar los archivos de software. Preferiblemente, el segundo servidor 200 verifica en primer lugar, con el fin de permitir la grabación/registro de los certificados digitales, que el propietario de certificado 300 se encuentra en posesión del certificado digital y que es capaz de realizar el proceso de firma de archivos. Este procedimiento valida los datos incluidos en el certificado digital (dominio, dirección electrónica o correo electrónico, etc.) en el caso de que un atacante 400 pudiera haber comprometido la infraestructura de web y de correos electrónicos del distribuidor de software y la PKI del cliente para hacerse pasar por un distribuidor de software legítimo 300.

Además, adicionalmente pueden realizarse varias verificaciones con el fin de certificar la relación de un nuevo certificado digital con la cuenta de un distribuidor de software existente 300. Esta labor se realiza con la introducción de un segundo factor del proceso de autenticación, por lo tanto antes de que se grabe un nuevo certificado digital en el segundo servidor 200, se realizan diferentes pruebas para validar la confiabilidad del certificado digital.

Además, pueden comprobarse una cadena de certificados de confianza y el estado de revocación y de caducidad del certificado digital que va a grabarse. En consecuencia, si hay cualquier anomalía un sistema de alerta en el segundo servidor 200 genera una notificación al distribuidor de software 300. Específicamente, una vez que la cadena de certificados de confianza se obtiene para el certificado particular, la relación entre la totalidad de las autoridades de certificación intermedias se analiza por medio de búsqueda de irregularidades.

Con el fin de lograr los fines que se han descrito en secciones previas, se presentan varias realizaciones. La primera realización se corresponde con el procedimiento básico que permite que el distribuidor de software 300 publique un certificado digital con el segundo servidor 200. Este procedimiento asocia este certificado digital con la cuenta del distribuidor de software y permite que el distribuidor de software 300 solicite el registro de archivos firmados demandando la creación de indicación de función de troceo. El resto de las realizaciones introducidas describen cómo se consiguen los fines avanzados por la presente invención.

Con referencia a la Figura 3, se muestra un proceso que puede seguirse para efectuar el registro de los certificados digitales empleados por el primer servidor 300 (o distribuidor de software debido a que los archivos de software se firman por el distribuidor de software a través de dicho primer servidor) para firmar de manera digital sus archivos. En la Figura 3, una vez que el distribuidor de software 300 ha solicitado su inicio de sesión por el segundo servidor (A), el segundo servidor 200 ha de verificar el nombre de usuario y la contraseña que se recibe (B). El segundo servidor 200 también puede iniciar un intercambio de un segundo factor de la autenticación. El primer lugar, el segundo servidor 200 genera un testigo que va a usarse como contraseña de un solo uso (OTP) (C) y envía entonces esta OTP al distribuidor de software 300 usando un canal diferente del que usa normalmente. En la presente invención se propone el uso de varios canales (SMS, correo electrónico, etc.) para su uso por el distribuidor de software 300 para recibir esta OTP 302. Una vez que se recibe, el distribuidor de software 300 introduce la OTP en la interfaz 301 y envía esta (G) al segundo servidor 200. El segundo servidor comprueba si la OTP coincide con la que se ha generado con anterioridad. Si el proceso de coincidencia devuelve resultados positivos, el segundo servidor 200 confirma el inicio de sesión al distribuidor de software 300 (I). Entonces, el distribuidor de software 300 solicita, usando un navegador web 301, la adscripción de un nuevo certificado digital enviando el propio certificado dentro de la solicitud (J). Una vez que el certificado digital se ha recibido, el segundo servidor 200 realiza un análisis exhaustivo del certificado digital (K), verificando si este es un certificado digital emitido que va a usarse en los procesos de firma de códigos y comprobando si su estado más recientemente actualizado está establecido como revocado o como caducado. Los procedimientos definidos para realizar estos análisis de aprovechan de las técnicas habituales propuestas para estas tareas. Si el certificado digital recibido es un certificado de firma válido, el segundo servidor 200 determina qué cadena de confianza permite certificar la autoridad de certificación emisora como válida (L). Por otro lado, esta cadena se considera como válida si no hay anomalía alguna entre las autoridades de certificación que participan en la cadena. Una vez que se ha establecido la relación completa de las autoridades de certificación necesarias para alcanzar la autoridad raíz, el segundo servidor fija esta con el fin de crear una huella digital de certificado. Entonces, el segundo servidor 200 almacena esta huella digital de certificado además del

nuevo certificado digital, ambos en relación con la cuenta de usuario (M).

Si se detectó cualquier anomalía cuando se había analizado la cadena de certificados de confianza, el segundo servidor 200 genera una alerta para informar al distribuidor de software 300 de que es probable que haya existido una autoridad de certificación comprometida cuando el certificado se emitió.

Una vez que un distribuidor de software 300 tiene por lo menos un certificado digital registrado con el segundo servidor 200, este puede comenzar a registrar la información en relación con la firma de sus archivos de software (archivos binarios o archivos de documento). Se hará referencia a esta información como indicación de función de troceo. Con referencia a la Figura 4, una vez que un distribuidor de software 300 se ha autenticado correctamente (A y B1) por el segundo servidor 200, este último ha de verificar que el archivo de software seleccionado que ha de registrarse usando el segundo servidor 200 es el archivo de software esperado y que este se ha firmado usando un certificado digital (C) registrado con anterioridad. Entonces, de acuerdo con una primera alternativa, usando el programa especializado de un distribuidor de software, 300 puede extraer los contenidos de firma a partir del archivo de software firmado (D). La norma que se emplea habitualmente para almacenar estos contenidos de firma se denomina PKCS y mantiene, en una estructura de datos, la totalidad de la información necesaria para verificar la firma digital de un archivo de software (certificado digital usado, se ha aplicado función de troceo, resumido, etc.). El distribuidor de software 300 envía este PKCS junto con el nombre de archivo de software para solicitar la generación de indicación de función de troceo para el archivo de software analizado (E). Una vez que el segundo servidor 200 recibe esta solicitud, este extrae el certificado del distribuidor de software a partir de los datos en la solicitud y verifica si está relacionado con anterioridad con el distribuidor de software 300 que se ha autenticado (F). Cuando el segundo servidor 200 verifica que el PKCS se corresponde con un cliente legitimado, este recupera la cadena de certificados de confianza prefijada para el certificado digital particular (G) y obtiene la cadena de confianza que puede fijarse en el momento en el que se está evaluando la solicitud. El segundo servidor 200 verifica entonces si existe diferencia alguna que pudiera alertar acerca de la posibilidad de una sustitución ilegal de una autoridad de certificación. Si todo es correcto, el segundo servidor 200 almacena entonces los contenidos de la solicitud (I) y genera la indicación de función de troceo que incluye el resumen al que se ha aplicado función de troceo del archivo de software, el certificado digital usado en la firma digital y un sello de tiempo generado por el segundo servidor 200 (J). De hecho, este resumen al que se ha aplicado función de troceo se usa para indizar la indicación de función de troceo generada en el sistema.

Con referencia a la Figura 5 una segunda alternativa se presenta para resolver el mismo proceso. La diferencia principal entre esta nueva realización y la que se describe en la Figura 4 es que ahora, una vez que el distribuidor de software 300 se ha autenticado (A y B1), el distribuidor de software 300 firma de manera digital el archivo de software y carga este al segundo servidor 200 (D). En este caso, es el segundo servidor 200 el que se encuentra a cargo de extraer el PKCS a partir del archivo de software. Entonces, el segundo servidor 200 extrae el certificado del distribuidor de software a partir de los datos en el PKCS (E) y verifica si está relacionado con anterioridad con el distribuidor de software 300 que se ha autenticado (F). Cuando el segundo servidor 200 verifica que la información contenida en el PKCS se corresponde con un cliente legitimado, este verifica la corrección de la firma digital (G) y obtiene la cadena de confianza que puede fijarse en el momento en el que se está evaluando la solicitud (H). El segundo servidor 200 verifica entonces si existe diferencia alguna entre esta cadena de confianza y la cadena de certificados de confianza prefijada para el certificado digital particular (I), si esta existe el sistema puede alertar acerca de la posibilidad de una sustitución ilegal de una autoridad de certificación. Si todo es correcto, el segundo servidor 200 almacena entonces los contenidos de la solicitud (J) y genera la indicación de función de troceo que incluye el resumen al que se ha aplicado función de troceo del archivo, el certificado digital usado en la firma digital y un sello de tiempo generado por el segundo servidor (K). De nuevo, este resumen al que se ha aplicado función de troceo se usa para indizar la indicación de función de troceo generada en el sistema.

Una vez que se ha generado la indicación de función de troceo de un archivo de software firmado, el usuario final 100 puede verificar si sus copias adquiridas del archivo coinciden con el archivo de software registrado con el segundo servidor 200. Incluso, los usuarios finales pueden verificar si el distribuidor de software esperado 300 fue en realidad quien firmó el archivo de software y cuándo firmó este el archivo de software.

Con referencia a la Figura 6, se presenta una realización que explica cómo un usuario 100 puede verificar el estado de archivo de software firmado. Una vez que el usuario 100 ha realizado las comprobaciones habituales con el fin de validar la firma digital (A), el programa especializado de un usuario puede usarse para extraer el PKCS a partir del archivo de software (B) y enviar una solicitud de validación de indicación de función de troceo al segundo servidor 200 (C). Cuando el segundo servidor 200 recibe esta solicitud, puede extraer el certificado digital a partir del PKCS en la solicitud (D). Si este certificado digital se ha registrado en el sistema, el segundo servidor 200 puede recuperar el resumen al que se ha aplicado función de troceo a partir del PKCS también (E). Usando esta función de troceo como índice, puede devolver la totalidad de la información almacenada durante la generación de la indicación de función de troceo (F). Esta información permite que el segundo servidor 200 verifique la cadena de certificados de confianza (G, H e I) y determine el estado de certificado en comparación con el certificado almacenado durante el registro de certificado digital (J).

Con referencia a la Figura 7, se describe otra realización para dejar que los usuarios 100 verifiquen sus archivos adquiridos cargando la totalidad del archivo de software firmado. En este caso, la primera etapa realizada por el usuario 100 es cargar el archivo de software firmado al segundo servidor 200 (A). Una vez que se recibe el archivo de software firmado, el segundo servidor 200 ejecuta las comprobaciones habituales con el fin de verificar la corrección de la firma de archivo (B). A partir de este punto, el segundo servidor 200 extrae el certificado a partir del PKCS para comprobar si este se corresponde con un distribuidor de software válido 300 (C). Este extrae el resumen al que se ha aplicado función de troceo para realizar una búsqueda indizada de la información en relación con el archivo de software analizado (D y E). Extrayendo este certificado digital (F), el segundo servidor 200 obtiene la cadena de certificados de confianza (G) y compara esta con la cadena de certificados de confianza almacenada durante dicho registro de certificado digital (H) para decidir si el archivo de software es, de hecho, un archivo de confianza.

De acuerdo con otra realización más, el segundo servidor 200 puede aprovechar la información que se proporciona por diversas fuentes oficiales remotas tal como una autoridad de certificación (CA) o un protocolo de estado de certificado en línea (OCSP) para comprobar el estado del certificado digital. Este también puede ejecutar un rastreador web para buscar diferentes instancias del archivo de software firmado en la web. En consecuencia, si se encuentra una de estas instancias, un procedimiento de verificación de firma se ejecuta sobre este archivo. El segundo servidor 200 informará al distribuidor de software 300 y forzará la revocación del certificado digital sospechoso en el caso de ser un certificado digital comprometido. El segundo servidor 200 también informará a los usuarios 100 que solicitan información en relación con estos archivos de software de que los archivos de software no son dignos de confianza.

El alcance de la presente invención se define en el siguiente conjunto de reivindicaciones.

REIVINDICACIONES

1. Un método implementado por ordenador para evitar problemas de seguridad en el uso de certificados digitales en la firma de códigos, que comprende:

- firmar, por un distribuidor de software a través de un primer servidor (300), por lo menos un archivo de software usando un certificado digital con una firma digital que identifica a dicho distribuidor de software; y
- adquirir, por al menos un usuario (100) a través de un dispositivo de cálculo, una copia de dicho por lo menos un archivo de software firmado; y
- generar, mediante un segundo servidor (200) en comunicación con dicho primer servidor (300), tras una petición hecha por el distribuidor de software, una indicación de función de troceo del al menos un archivo de software firmado,

dicho método implementado por ordenador, en el que, antes de que el segundo servidor reciba la petición,

- dicho certificado digital a usar para dicha firma se graba en dicho segundo servidor (200), estando el certificado digital a grabar proporcionado por el distribuidor de software (300) tras el registro de este último en dicho segundo servidor (200) e incluyendo el certificado digital información obtenida de una cadena de certificado de confianza asociada al certificado digital cuando realiza dicho registro, en el que dicho registro comprende comprobar, por el segundo servidor (200), datos incluidos en el certificado digital proporcionado que incluye al menos un dominio y/o una dirección electrónica; y en el que dicho registro comprende además:

  - realizar, por el segundo servidor (200), una autenticación de dicho certificado digital realizando las siguientes etapas:
  - generar una contraseña de un solo uso, OTP;
  - enviar, dicha OTP generada al distribuidor de software (300) a través de un canal de comunicación que incluye al menos un mensaje de texto, un mensaje electrónico o un mensaje instantáneo; y
  - certificar, tras la recepción de dicha OTP desde el distribuidor de software (300), que la OTP recibida coincide con dicha OTP generada, y en que:

- dicha indicación de función de troceo incluye información acerca del distribuidor de software (300) y acerca del archivo de software firmado y un registro de tiempo que certifica un momento en el que se notifica la firma del archivo de software al distribuidor de software (300).

2. El método de la reivindicación 1, en el que dicha indicación de función de troceo se genera tras la recepción desde el distribuidor de software (300) de:

- la firma digital del archivo de software firmado junto con un nombre del archivo de software firmado, extrayéndose la firma digital a partir del archivo de software firmado por medio de un programa especializado del distribuidor de software (300); o
- una carga directa del archivo de software firmado, extrayendo el segundo servidor (200) la firma digital a partir del archivo cargado y verificando adicionalmente la misma.

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

- comprobar el estado de revocación y de caducidad del certificado digital proporcionado; y
- en el caso de que dicho estado de revocación y de caducidad se compruebe como válido, certificar la corrección de dicha cadena de certificados de confianza.

4. El método de la reivindicación 1, en el que el segundo servidor (200) comprueba periódicamente un estado del certificado digital grabado usando una información que se proporciona a partir de fuentes remotas que incluyen por lo menos uno de una autoridad de certificación (CA) o un protocolo de estado de certificado en línea (OCSP).

5. El método de la reivindicación 4, en el que el segundo servidor (200) busca además ejecutando un motor de metabúsqueda para una pluralidad de diferentes instancias del archivo de software firmado en una web.

6. El método de cualquiera de las reivindicaciones anteriores 4 o 5, en el que, en el caso de que se encuentre una anomalía con respecto a un estado no válido del certificado digital grabado y/o de que se encuentre una instancia en dicha web, el segundo servidor (200) por lo menos informa al distribuidor de software (300) acerca de dicha anomalía encontrada, revocando este último el certificado digital grabado a partir del segundo servidor (200) en el caso de ser un certificado digital comprometido.

7. El método de la reivindicación 1, en el que el segundo servidor (200) informa además a dicho por lo menos un usuario (100) acerca de dicha anomalía encontrada.

8. El método de la reivindicación 1, que además comprende verificar, por dicho por lo menos un usuario (100), que

dicha copia adquirida del archivo de software firmado coincide con dicho archivo de software firmado al que se ha aplicado indicación de función de troceo:

- comprobando, el por lo menos un usuario (100), la validez de la firma digital de la copia adquirida del archivo de software firmado;
- extrayendo, el por lo menos un usuario (100) usando un programa especializado, datos de firma a partir de la copia adquirida del archivo de software firmado y solicitando una validación de indicación de función de troceo al segundo servidor (200); y
- recuperando, por el segundo servidor (200), un resumen al que se ha aplicado función de troceo usando este último como un índice y devolviendo al por lo menos un usuario (100) una información con respecto a dicha indicación de función de troceo.

9. El método de la reivindicación 1 u 8, que además comprende probar, por dicho por lo menos un usuario (100), la autoría y la fecha de dicha firma realizando el segundo servidor (200) las siguientes etapas:

- comprobar, tras la recepción de la copia adquirida del archivo de software firmado a partir del por lo menos un usuario (100), la validez de la firma digital de dicha copia adquirida;
- extraer, datos de firma a partir de la copia adquirida del archivo de software firmado y comprobar que se corresponde con el distribuidor de software (300);
- recuperar, un resumen al que se ha aplicado función de troceo y usar este último como un índice para buscar información de indicación de función de troceo con respecto a la copia adquirida; y
- comparar una cadena de certificados de confianza obtenida de la copia adquirida con una cadena de certificados de confianza del archivo de software firmado registrado.

10. Un sistema informático para evitar problemas de seguridad en el uso de certificados digitales en firma de códigos, que comprende:

- un primer servidor usado por un distribuidor de software (300) configurado para firmar al menos un archivo de software usando un certificado digital con una firma digital de dicho distribuidor de software (300);
- al menos un dispositivo informático de usuario de un usuario (100) para adquirir una copia de dicho al menos un archivo de software firmado; y
- un segundo servidor (200) en comunicación con dicho primer servidor (300), comprendiendo dicho segundo servidor (200) medios para generar una indicación de función de troceo, tras una petición hecha por el distribuidor de software (300), del al menos un archivo de software firmado,

dicho sistema informático en que:

- estando dicho segundo servidor (200) configurado, antes de recibir la petición, para grabar dicho certificado digital a usar por dicha firma, estando el certificado digital a grabar proporcionado por el distribuidor de software (300) tras el registro de este último en dicho segundo servidor (200) e incluyendo el certificado digital información obtenida de una cadena de certificado de confianza asociada al certificado digital cuando realiza dicho registro, en el que el segundo servidor (200) comprende medios para registrar el distribuidor de software (300) comprobando datos incluidos en el certificado digital proporcionado que incluye al menos un dominio y/o una dirección electrónica y realizando además una autenticación del certificado digital:
  - generando una contraseña de un solo uso, OTP;
  - enviando, dicha OTP generada al distribuidor de software (300) a través de un canal de comunicación que incluye al menos un mensaje de texto, un mensaje electrónico o un mensaje instantáneo; y
  - certificando, tras la recepción de dicha OTP desde el distribuidor de software (300), que la OTP recibida coincide con dicha OTP generada; y
  - en el que dicha indicación de función de troceo incluye información acerca del distribuidor de software (300) y acerca del archivo de software firmado y un registro de tiempo que certifica un momento en el que se notifica la firma del archivo de software al distribuidor de software (300).

11. El sistema de la reivindicación 10, que además comprende unos medios para usar una información que se proporciona a partir de fuentes remotas que incluyen por lo menos uno de una autoridad de certificación, CA, (CA) o un protocolo de estado de certificado en línea, OCSP, y/o unos medios para ejecutar un motor de metabúsqueda en una web.

12. Un producto de programa informático que comprende unos medios de código de programa informático que están adaptados para realizar las etapas de acuerdo con el método de la reivindicación 1 cuando dicho programa se ejecuta en un ordenador, un procesador de señales digitales, un campo de matrices de puertas programables, un circuito integrado específico de la aplicación, un microprocesador, un microcontrolador o cualquier otra forma de hardware programable.

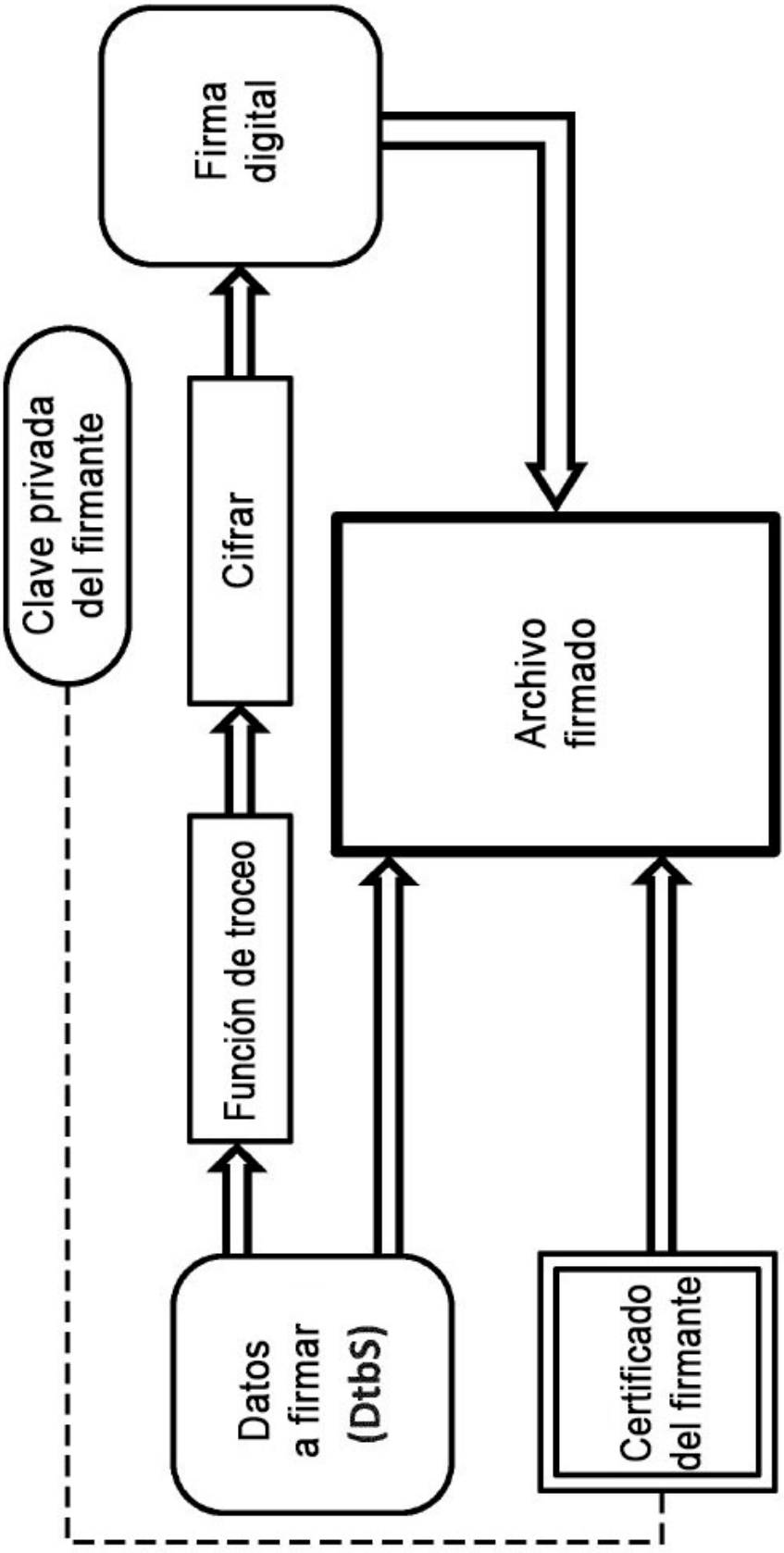
Firma digital
Clave privada del firmante
Cifrar
Archivo firmado
Función de troceo
Datos a firmar (DtbS)
Certificado del firmante

FIG. 1

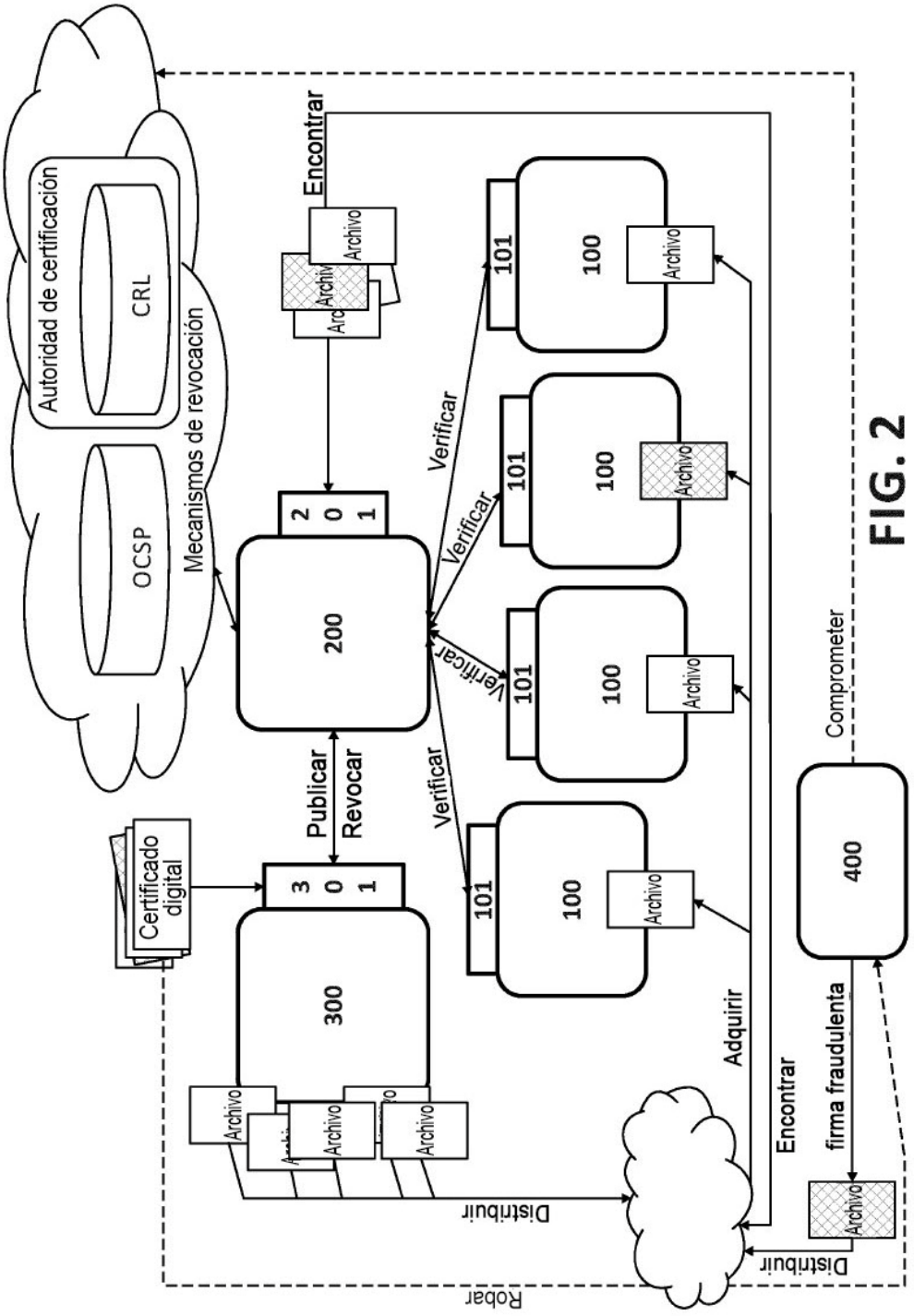
Autoridad de certificación
CRL
OCSP
Mecanismos de revocación
Encontrar
Archivo
200
201
Verificar
101
100
Publicar
Revocar
300
301
Certificado digital
Distribuir
Adquirir
Encontrar
firma fraudulenta
400
Comprometer
Robar

FIG. 2

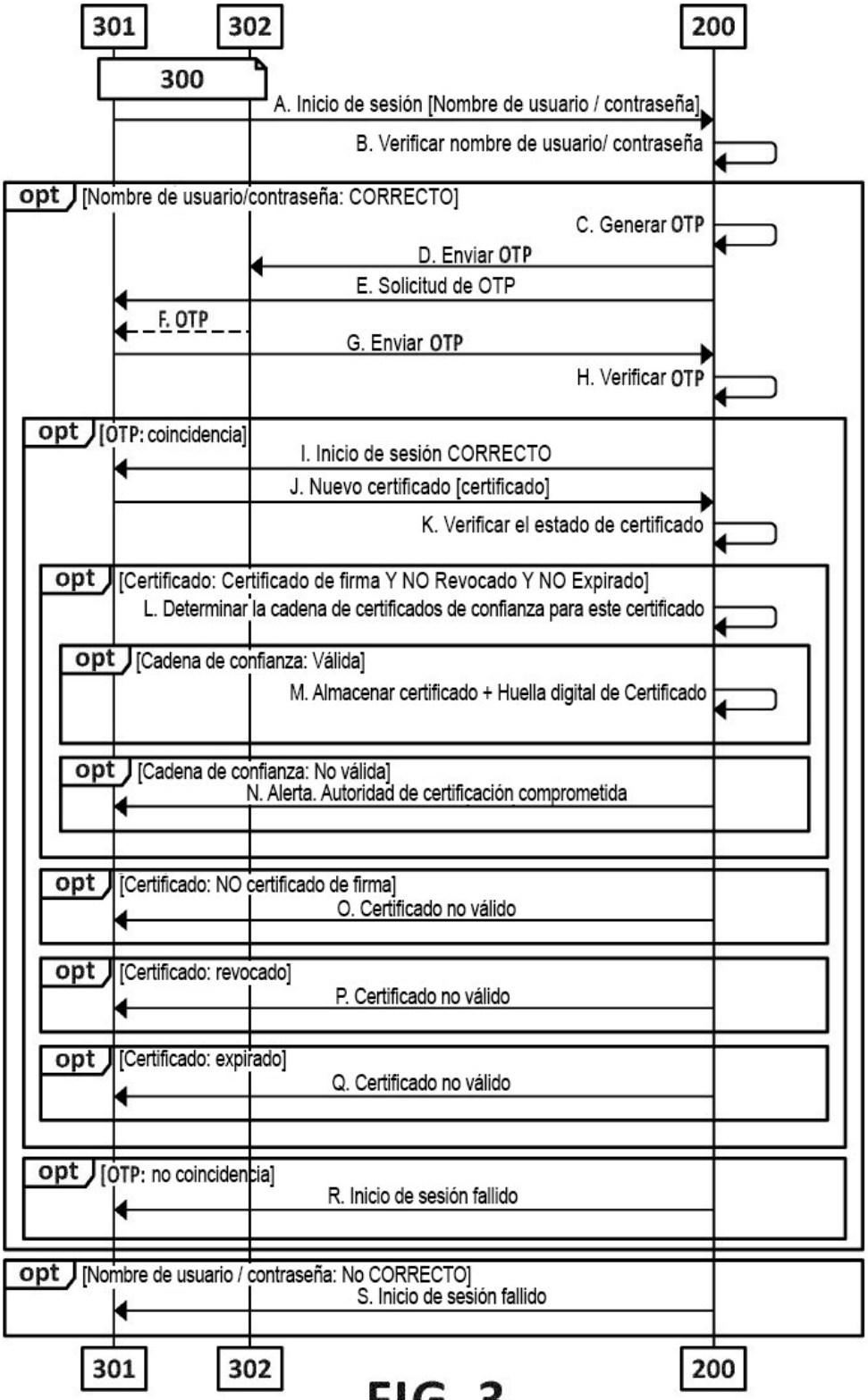
301
302
200
300
A. Inicio de sesión [Nombre de usuario / contraseña]
B. Verificar nombre de usuario/ contraseña
opt [Nombre de usuario/contraseña: CORRECTO]
C. Generar OTP
D. Enviar OTP
E. Solicitud de OTP
F. OTP
G. Enviar OTP
H. Verificar OTP
opt [OTP: coincidencia]
I. Inicio de sesión CORRECTO
J. Nuevo certificado [certificado]
K. Verificar el estado de certificado
opt [Certificado: Certificado de firma Y NO Revocado Y NO Expirado]
L. Determinar la cadena de certificados de confianza para este certificado
opt [Cadena de confianza: Válida]
M. Almacenar certificado + Huella digital de Certificado
opt [Cadena de confianza: No válida]
N. Alerta. Autoridad de certificación comprometida
opt [Certificado: NO certificado de firma]
O. Certificado no válido
opt [Certificado: revocado]
P. Certificado no válido
opt [Certificado: expirado]
Q. Certificado no válido
opt [OTP: no coincidencia]
R. Inicio de sesión fallido
opt [Nombre de usuario / contraseña: No CORRECTO]
S. Inicio de sesión fallido
301
302
200

FIG. 3

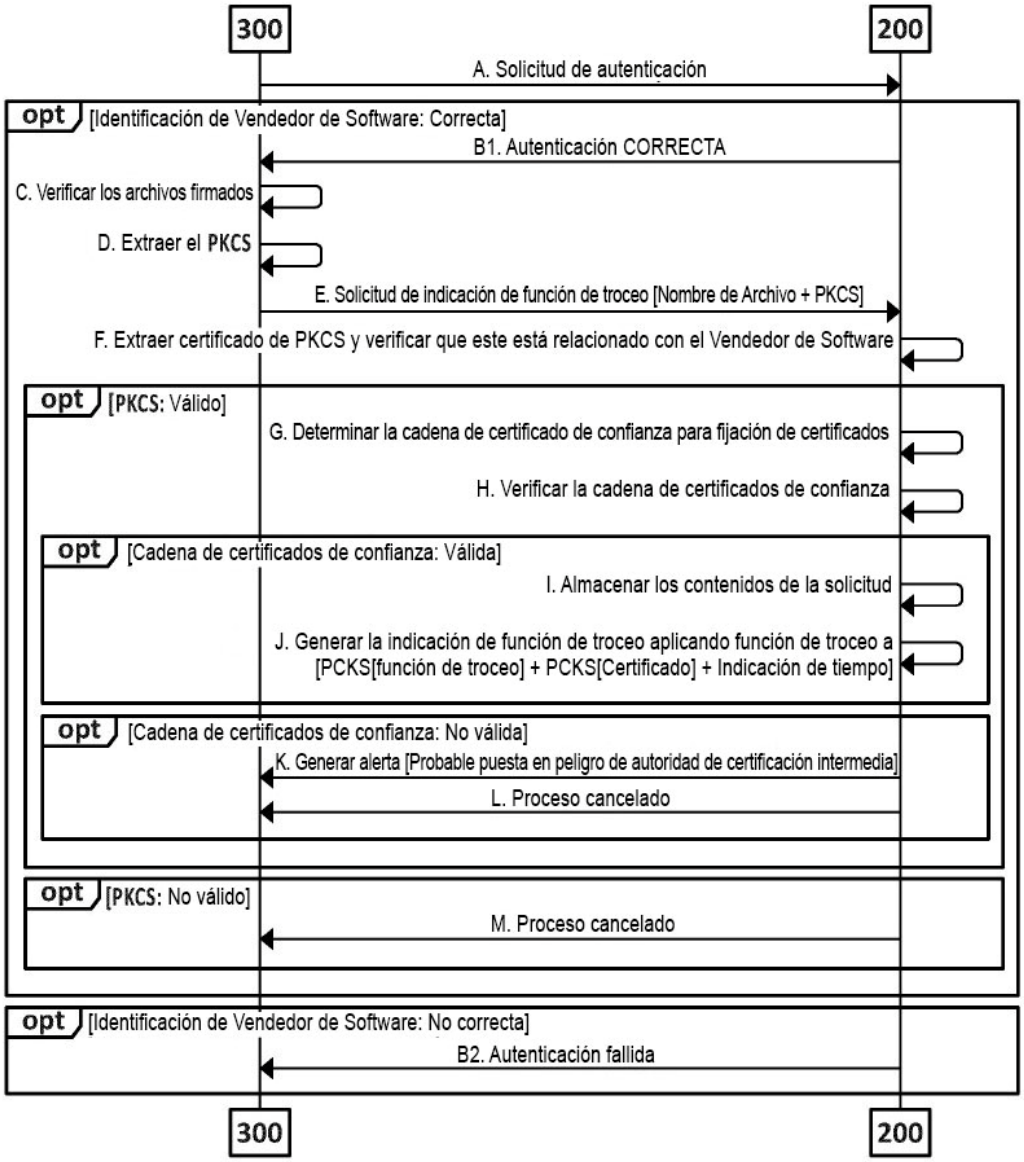
300
200
A. Solicitud de autenticación
opt [Identificación de Vendedor de Software: Correcta]
B1. Autenticación CORRECTA
C. Verificar los archivos firmados
D. Extraer el PKCS
E. Solicitud de indicación de función de troceo [Nombre de Archivo + PKCS]
F. Extraer certificado de PKCS y verificar que este está relacionado con el Vendedor de Software
opt [PKCS: Válido]
G. Determinar la cadena de certificado de confianza para fijación de certificados
H. Verificar la cadena de certificados de confianza
opt [Cadena de certificados de confianza: Válida]
I. Almacenar los contenidos de la solicitud
J. Generar la indicación de función de troceo aplicando función de troceo a [PCKS[función de troceo] + PCKS[Certificado] + Indicación de tiempo]
opt [Cadena de certificados de confianza: No válida]
K. Generar alerta [Probable puesta en peligro de autoridad de certificación intermedia]
L. Proceso cancelado
opt [PKCS: No válido]
M. Proceso cancelado
opt [Identificación de Vendedor de Software: No correcta]
B2. Autenticación fallida
300
200

FIG. 4

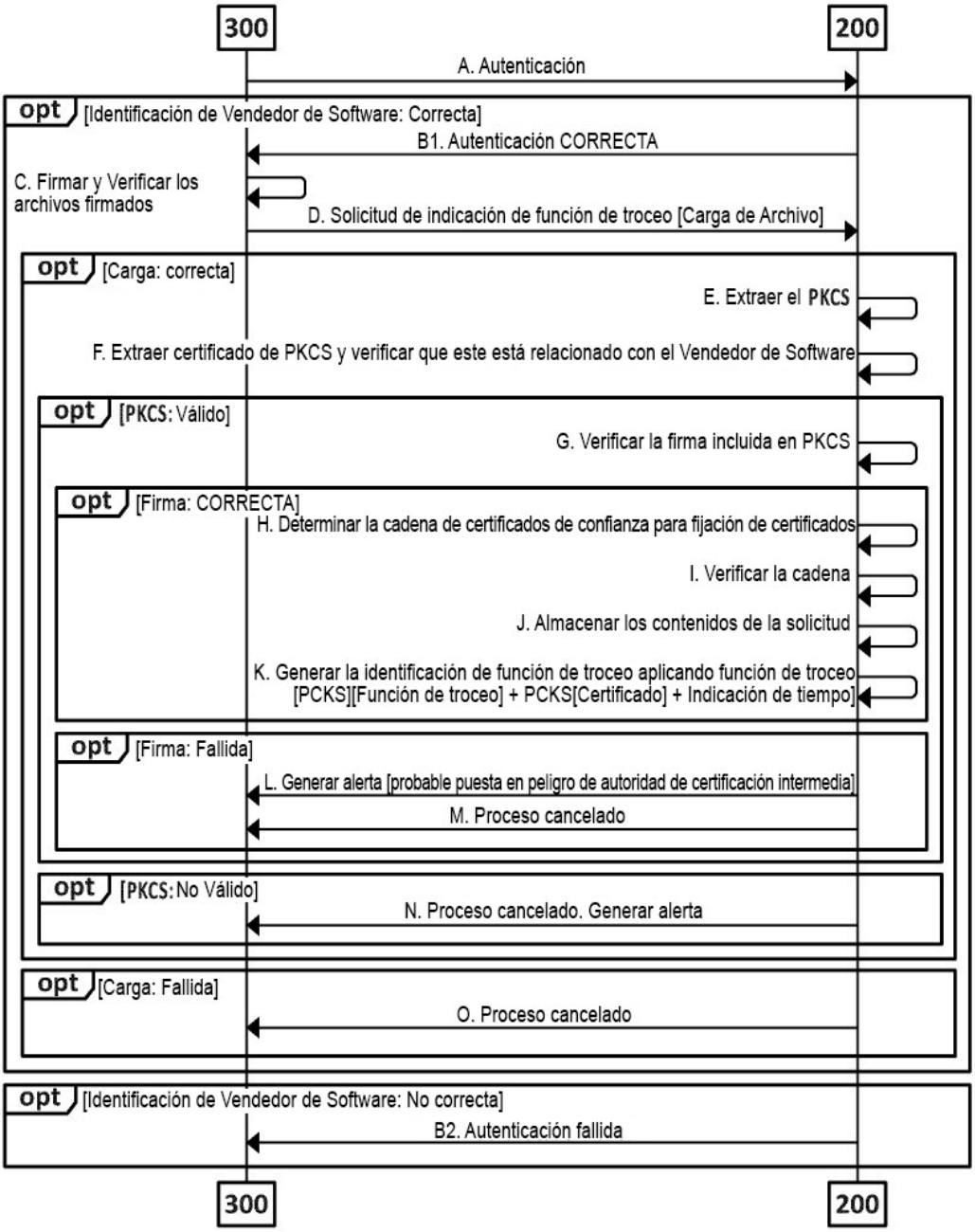
300
200
A. Autenticación
opt [Identificación de Vendedor de Software: Correcta]
B1. Autenticación CORRECTA
C. Firmar y Verificar los archivos firmados
D. Solicitud de indicación de función de troceo [Carga de Archivo]
opt [Carga: correcta]
E. Extraer el PKCS
F. Extraer certificado de PKCS y verificar que este está relacionado con el Vendedor de Software
opt [PKCS: Válido]
G. Verificar la firma incluida en PKCS
opt [Firma: CORRECTA]
H. Determinar la cadena de certificados de confianza para fijación de certificados
I. Verificar la cadena
J. Almacenar los contenidos de la solicitud
K. Generar la identificación de función de troceo aplicando función de troceo [PCKS][Función de troceo] + PCKS[Certificado] + Indicación de tiempo]
opt [Firma: Fallida]
L. Generar alerta [probable puesta en peligro de autoridad de certificación intermedia]
M. Proceso cancelado
opt [PKCS: No Válido]
N. Proceso cancelado. Generar alerta
opt [Carga: Fallida]
O. Proceso cancelado
opt [Identificación de Vendedor de Software: No correcta]
B2. Autenticación fallida
300
200

FIG. 5

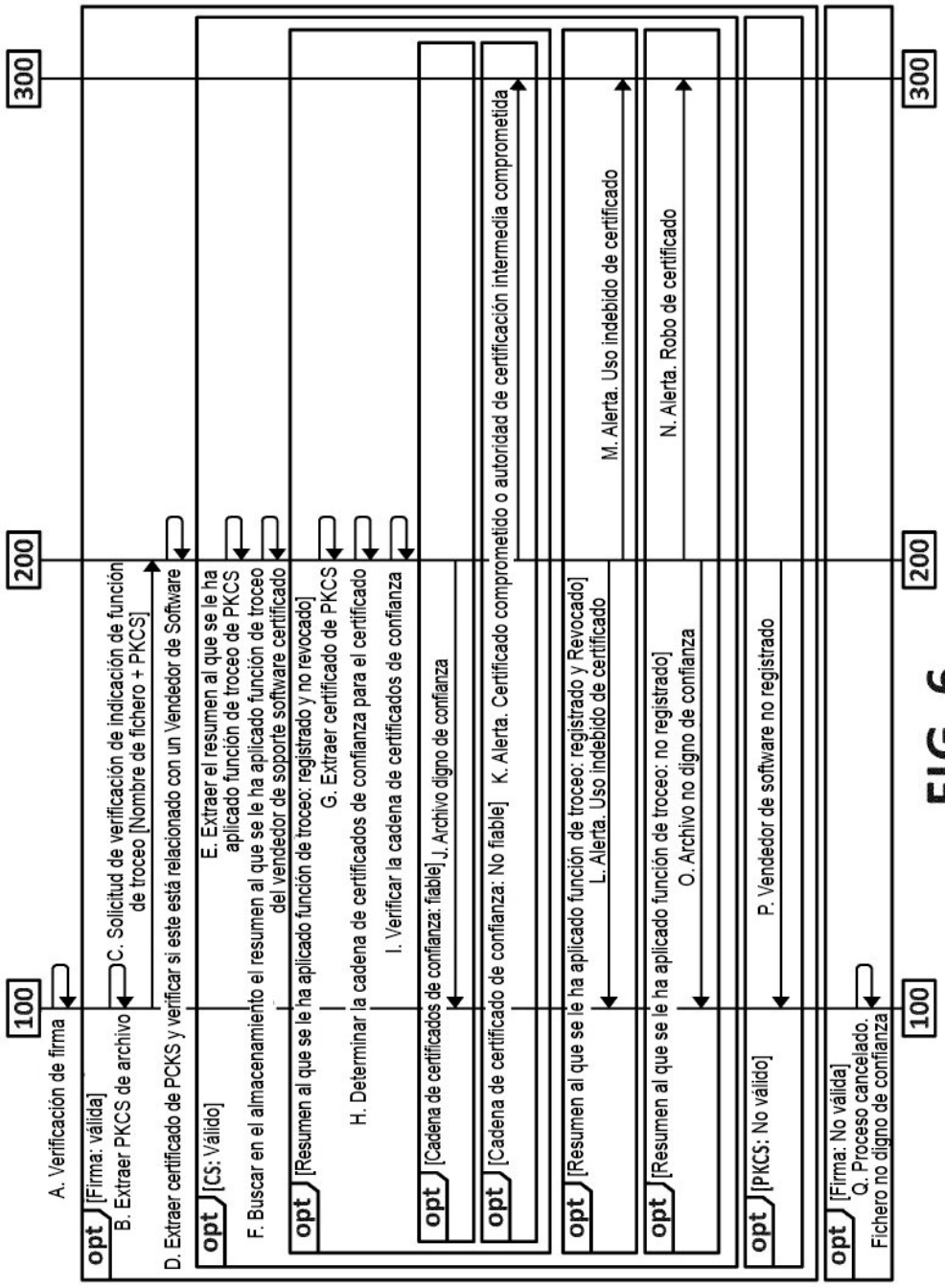
100
200
300
A. Verificación de firma
opt [Firma: válida]
B. Extraer PKCS de archivo
C. Solicitud de verificación de indicación de función de troceo [Nombre de fichero + PKCS]
D. Extraer certificado de PCKS y verificar si este está relacionado con un Vendedor de Software
opt [CS: Válido]
E. Extraer el resumen al que se le ha aplicado función de troceo de PKCS
F. Buscar en el almacenamiento el resumen al que se le ha aplicado función de troceo del vendedor de soporte software certificado
opt [Resumen al que se le ha aplicado función de troceo: registrado y no revocado]
G. Extraer certificado de PKCS
H. Determinar la cadena de certificados de confianza para el certificado
I. Verificar la cadena de certificados de confianza
opt [Cadena de certificados de confianza: fiable] J. Archivo digno de confianza
opt [Cadena de certificado de confianza: No fiable] K. Alerta. Certificado comprometido o autoridad de certificación intermedia comprometida
opt [Resumen al que se le ha aplicado función de troceo: registrado y Revocado]
L. Alerta. Uso indebido de certificado
M. Alerta. Uso indebido de certificado
opt [Resumen al que se le ha aplicado función de troceo: no registrado]
O. Archivo no digno de confianza
N. Alerta. Robo de certificado
opt [PKCS: No válido]
P. Vendedor de software no registrado
opt [Firma: No válida]
Q. Proceso cancelado. Fichero no digno de confianza

FIG. 6

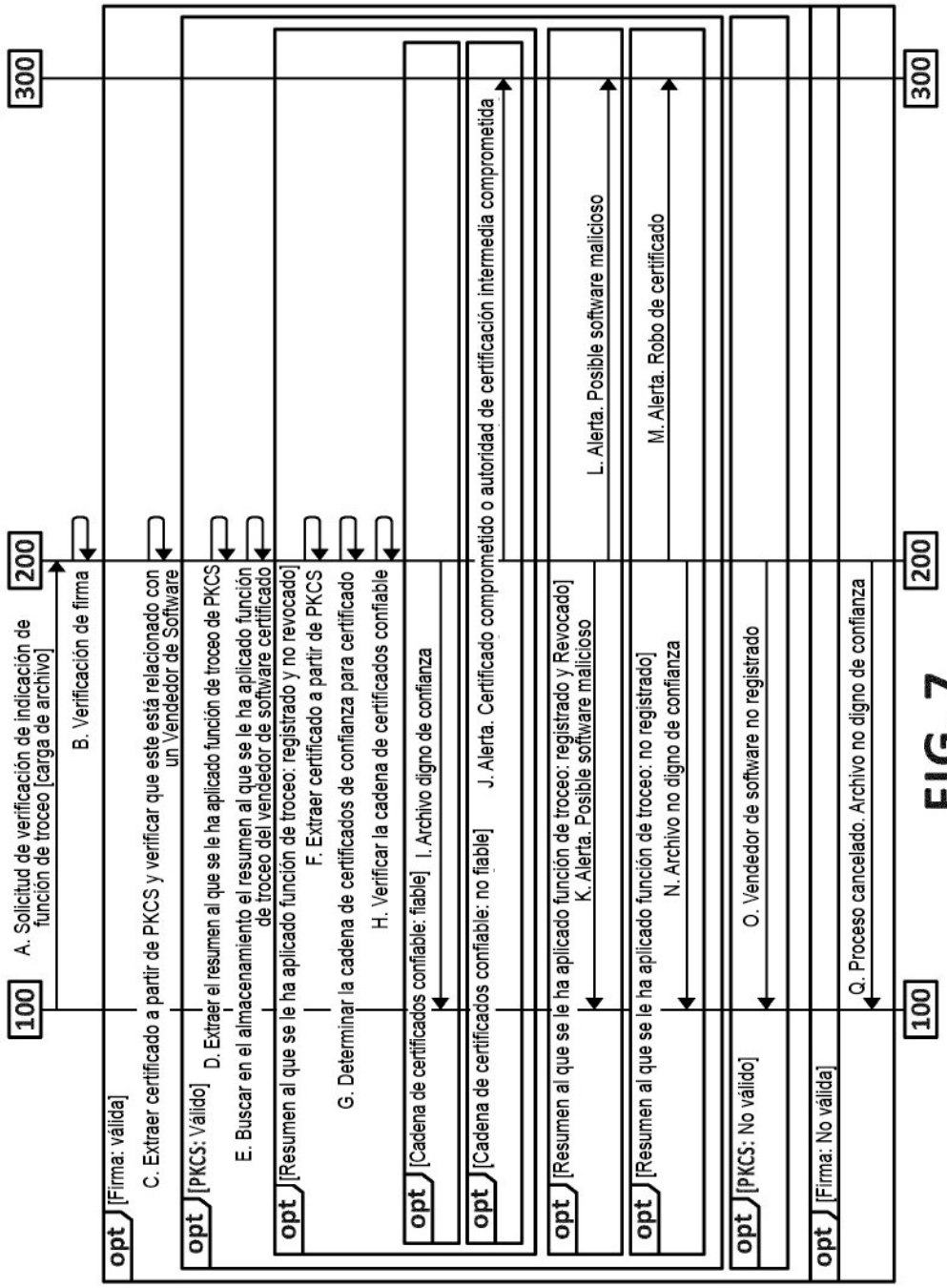
100
200
300
A. Solicitud de verificación de indicación de función de troceo [carga de archivo]
B. Verificación de firma
opt [Firma: válida]
C. Extraer certificado a partir de PKCS y verificar que este está relacionado con un Vendedor de Software
opt [PKCS: Válido]
D. Extraer el resumen al que se le ha aplicado función de troceo de PKCS
E. Buscar en el almacenamiento el resumen al que se le ha aplicado función de troceo del vendedor de software certificado
opt [Resumen al que se le ha aplicado función de troceo: registrado y no revocado]
F. Extraer certificado a partir de PKCS
G. Determinar la cadena de certificados de confianza para certificado
H. Verificar la cadena de certificados confiable
opt [Cadena de certificados confiable: fiable]
I. Archivo digno de confianza
opt [Cadena de certificados confiable: no fiable]
J. Alerta. Certificado comprometido o autoridad de certificación intermedia comprometida
opt [Resumen al que se le ha aplicado función de troceo: registrado y Revocado]
K. Alerta. Posible software malicioso
L. Alerta. Posible software malicioso
opt [Resumen al que se le ha aplicado función de troceo: no registrado]
N. Archivo no digno de confianza
M. Alerta. Robo de certificado
opt [PKCS: No válido]
O. Vendedor de software no registrado
opt [Firma: No válida]
Q. Proceso cancelado. Archivo no digno de confianza

FIG. 7