(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 554 229**

(51) Int. CI.:

G06F 21/00 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.04.2010 E 10717939 (2)**

(97) Fecha y número de publicación de la concesión europea: **26.08.2015 EP 2425370**

(54) Título: **Procedimiento y aparato para crear un entorno de navegación web seguro con firma de privilegios**

(30) Prioridad:

27.04.2009 US 430750

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.12.2015

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
Attn: International IP Administration, 5775 Morehouse Drive
San Diego, California 92121, US

(72) Inventor/es:

KELLEY, BRIAN, HAROLD

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Procedimiento y aparato para crear un entorno de navegación web seguro con firma de privilegios

Campo de la invención

La presente invención se refiere generalmente a comunicaciones de red por ordenador y más específicamente a certificados digitales de navegación web.

Antecedentes

Las nuevas tecnologías de Internet prometen una mayor integración entre los dispositivos de comunicaciones y las aplicaciones basadas en servidor. Las aplicaciones cliente-servidor tienen muchas ventajas y son cada vez más populares. Dichas aplicaciones permiten que la mayoría de los datos de aplicación existan en una ubicación de un servidor, aumentando la seguridad de los datos y eliminando copias de datos redundantes innecesarias. De forma análoga, una mayor parte del código de programación de la aplicación y los archivos de datos puede existir en una ubicación donde se mantiene más fácilmente por los desarrolladores de aplicaciones. Adicionalmente, pueden diseñarse aplicaciones cliente-servidor tales que se produzcan tareas de procesamiento rigurosas en el lado del servidor, lo que permite que existan aplicaciones robustas en dispositivos más pequeños y menos potentes tales como ordenadores portátiles y terminales móviles.

El documento de la técnica anterior "Going Beyond the Sand box: An Overview of the New Security Architecture in the Java Development Kit 1.2" de Gong L. y col., PROCEEDINGS OF THE USENIX SYMPOSIUM ON INTERNET TECHNOLOGIES AND SYSTEMS, 1 de diciembre de 1997, pág. 1 a 10, se refiere a la arquitectura de seguridad en el kit de desarrollo Java 1.2. El código fuente comprende información de URL y puede usarse con un navegador web. Un fragmento de código se caracteriza completamente por su origen (su ubicación tal como se especifica por una dirección URL) y el conjunto de claves públicas que corresponden al conjunto de claves privadas que se han usado para firmar el código usando uno o más algoritmos de firma digital. Para un código fuente que coincida con una entrada dada en la política, tanto la información de URL como la información de la firma deben coincidir (por ejemplo, una clave pública correspondiente a una firma en el código fuente coincide con la clave de un firmante en la entrada de la política).

Las tecnologías cliente-servidor han evolucionado para incluir un código móvil, como se ilustra en JavaScript® integrado en HTML. Las capacidades de las aplicaciones basadas en web actualmente están limitadas por la falta de funcionalidad disponible para código móvil dentro del entorno de ejecución del lado del cliente. Aunque los lenguajes tales como JavaScript® podrían diseñarse para permitir una funcionalidad avanzada en el lado del cliente, una implementación tal no es ideal desde un punto de vista de la seguridad. En un entorno donde la seguridad no es una preocupación, las aplicaciones basadas en servidor personalizarán el contenido basado en ubicación, sincronizarán archivos remotos con archivos del cliente y enlazarán la funcionalidad de escritorio con las funciones basadas en servidor. Sin embargo, los usuarios de Internet generalmente no son lo suficientemente sofisticados como para tomar decisiones informadas sobre si permitir a los sitios Web acceder a diversos recursos en el cliente. Esto se demuestra por la gran cantidad de productos diseñados para bloquear código malicioso de sitios web. Por lo tanto, cualquier avance en la funcionalidad de scripting basado en servidor podría hacer más daño que bien.

RESUMEN

En diversas realizaciones, se usan certificados digitales y firmas digitales para permitir que un dispositivo móvil determine si se le debería permitir a un servidor web obtener acceso a los diversos recursos en el dispositivo móvil. Los certificados digitales permiten a los dispositivos móviles y a los usuarios de dispositivos móviles saber la identidad de un servidor web, así como si ese servidor es de confianza para acceder a un recurso específico. Los dispositivos móviles pueden establecer la fiabilidad de un servidor web o de scripts descargados examinando el emisor del certificado digital presentado y pueden rastrear la fiabilidad a través de una cadena de certificados digitales con respecto a una autoridad inherentemente de confianza.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Los dibujos adjuntos, que se incorporan en el presente documento y constituyen parte de esta memoria descriptiva, ilustran realizaciones ejemplares de la invención y junto con la descripción general dada anteriormente y la descripción detallada dada a continuación, sirven para explicar las características de la invención.

La FIG. 1 es un diagrama de bloques del sistema de la red móvil inalámbrica.

La FIG. 2 es un diagrama de flujo de procesos de un procedimiento de la realización adecuado para determinar la fiabilidad de un script.

La FIG. 3A es un diagrama de flujo de procesos de un procedimiento de la realización para firmar digitalmente y

verificar un documento.

La FIG. 3B es un diagrama de flujo de procesos de un procedimiento de la invención adecuado para verificar certificados digitales.

La FIG. 3C es un diagrama de flujo de procesos de un procedimiento de realización alternativa adecuado para firmar digitalmente y verificar un documento.

Las FIG. 4A y B son diagramas de flujo de mensajes de realizaciones para establecer un entorno de navegación de confianza.

La FIG. 5 es un diagrama de flujo de procesos de un procedimiento de la realización adecuado para establecer un entorno de navegación de confianza.

La FIG. 6 es un diagrama de flujo de mensajes de una realización para establecer un entorno de navegación de confianza.

La FIG. 7 es un diagrama de bloques de circuito de un dispositivo móvil ejemplar adecuado para su uso con las diversas realizaciones.

La FIG. 8 es un diagrama de bloques de circuito de un ordenador personal ejemplar adecuado para su uso con las diversas realizaciones.

DESCRIPCIÓN DETALLADA

Las diversas realizaciones se describirán en detalle con referencia a los dibujos adjuntos. Siempre que sea posible, se usarán los mismos números de referencia a lo largo de los dibujos para referirse a las mismas partes o a partes similares. Las referencias hechas de ejemplos e implementaciones particulares son con fines ilustrativos y no pretenden limitar el alcance de la invención o las reivindicaciones.

Como se usa en el presente documento, las expresiones "terminal móvil", "móvil", "dispositivo móvil" y "dispositivo portátil" se refieren a uno cualquiera o todos los teléfonos móviles, asistentes personales de datos (PDA), ordenadores de bolsillo, receptores de correo electrónico inalámbricos y receptores de teléfonos móviles (por ejemplo, dispositivos Blackberry® y Treo®), teléfonos móviles con acceso a Internet multimedia (por ejemplo, el iPhone®) y dispositivos electrónicos personales similares que incluyen un procesador programable y una memoria y la capacidad de conectarse a una red inalámbrica. Los términos también pueden incluir ordenadores personales, tales como un ordenador portátil o un ordenador de sobremesa, cuando se usan en la descripción de las diversas realizaciones que también pueden implementarse en ordenadores personales. Aunque las diversas realizaciones se refieren a sistemas de red de telefonía móvil que incluyen torres celulares de dichas redes, el alcance de la presente invención y las reivindicaciones incluye cualquier sistema de comunicación que incluya células de comunicación inalámbrica distantes, incluyendo, por ejemplo, WiFi, WiMax y otras tecnologías de comunicación de red de datos inalámbricas, así como redes alámbricas, tales como LAN, WAN e Internet.

Como se usa en el presente documento, el término "script" se refiere a cualquier o todos los programas informáticos, incluyendo tanto programas informáticos escritos en un lenguaje de scripting tradicional, tales como JavaScript® o Perl®, que está diseñado para controlar un programa informático de ejecución como programas informáticos escritos en un lenguaje independiente, tales como C++ o Java® que se compila para su ejecución directamente en un sistema operativo o entorno de tiempo de ejecución.

Como se usan en el presente documento, los términos "navegador" y "navegador web" se refieren a cualquier entorno de tiempo de ejecución que sea capaz de ejecutar scripts o código, incluyendo navegadores tales como Internet Explorer® y Firefox®, entornos de tiempo de ejecución de lenguaje de programación, tal como un intérprete Perl® y el entorno de tiempo de ejecución binario para aplicaciones inalámbricas BREW®, así como sistemas operativos que incorporan capacidades de ejecución de script.

Como se usan en el presente documento, los términos "cliente" y "servidor" se refieren bien a un dispositivo, tal como un terminal móvil o un ordenador personal, con un procesador capaz de ejecutar un programa informático y un medio para comunicar con otros dispositivos que ejecutan programas informáticos tal como una conexión a Internet o un programa informático, o bien se refieren a un programa informático, tal como un navegador web o un sistema operativo, que incluye un enlace para comunicar con programas informáticos que se ejecutan en otros sistemas operativos, tal como una Conexión a Internet. Los términos "cliente" y "servidor" son de naturaleza descriptiva y no pretenden limitar el alcance de la invención o las reivindicaciones.

Los terminales móviles y ordenadores personales a menudo tienen navegadores web o tipos similares de programas que pueden ejecutar código descargado de sitios web. El navegador, junto con complementos y extensiones asociados, sirve como una puerta entre un terminal móvil y un sitio web. El sitio web puede presentar un script al

terminal móvil, pero el navegador es el programa que ejecuta el script. Por ejemplo, si un programa de correo electrónico basado en web solicita acceso al historial de llamadas del terminal móvil para relacionar los correos electrónicos con las llamadas del móvil, ello puede generar un script que solicita al navegador enviar una lista de llamadas al sitio web a través de una solicitud http. El navegador enviará una solicitud al sistema operativo del terminal móvil y el sistema operativo compilará la lista y la pasará al navegador.

Por supuesto, no todos los sitios web deberían tener acceso al historial de llamadas u otros tipos de datos personales y confidenciales alojados en un dispositivo móvil u ordenador personal. Se conocen bien los problemas de "hackers", sitios web maliciosos y otros abusos de Internet. Para la defensa de los ordenadores personales contra este tipo de ataques, están disponibles en el mercado muchos programas cortafuegos y se usan ampliamente para denegar el acceso a sitios web que no son de confianza. En los dispositivos móviles, tales como teléfonos móviles, los sitios web generalmente tienen bloqueado el acceso al sistema y los datos personales como parte del software del sistema operativo de los dispositivos. Aunque estos procedimientos impiden algunas aplicaciones muy útiles y servicios que de lo contrario podrían proporcionarse a través de Internet, dichas medidas son necesarias para proteger los dispositivos móviles contra el ataque por parte de sitios no fiables.

Las diversas realizaciones proporcionan procedimientos para establecer confianza entre un sitio web y un terminal móvil. Las diversas realizaciones hacen uno de los certificados digitales publicados por una autoridad de certificación que permite al terminal móvil confirmar la confianza en el sitio web o la confianza en el script emitido desde el sitio web. Una autoridad de certificación es una entidad de confianza que puede verificar que otra entidad es de confianza, como se demuestra por el certificado digital. Esto se conoce como una "cadena de confianza" o "encadenamiento de confianza". Una cadena de confianza debe proceder de una entidad de confianza. Las entidades que son inherentemente de confianza se denominan como autoridades principales. Un sistema operativo a menudo mantendrá un conjunto de certificados raíz o un "conjunto raíz", que son los certificados digitales de diversas autoridades principales.

Las diversas realizaciones pueden emplearse en una diversidad de redes alámbricas e inalámbricas, incluyendo, por ejemplo una red inalámbrica que emplea enlaces de comunicación de datos móviles. A modo de ejemplo, la FIG. 1 muestra un diagrama de bloques de una red de comunicación 10 que incluye Internet 24 y una red móvil en la que algunos dispositivos de comunicación, tales como los terminales móviles 28 y ordenadores personales 29, tienen la capacidad adicional de ejecutar scripts que se descargan de servidores web.

En esta red ejemplar 10, la estación base 16 es una parte de una red móvil que incluye elementos necesarios para el funcionamiento de la red, tal como un centro de conmutación móvil (MSC) 18. Durante el funcionamiento, el MSC 18 es capaz de enrutar llamadas y mensajes a y desde el terminal móvil 28 a través de la estación base 16 cuando el terminal móvil 28 está haciendo o recibiendo llamadas. El MSC 18 también proporciona una conexión a troncos de telefonía fija (no mostrado) cuando el terminal móvil 28 está involucrado en una llamada.

Además, el MSC puede acoplarse a una pasarela de servidor 22 acoplada a Internet 24. A través de la pasarela de servidor 22 el terminal móvil 28 puede comunicar con los servidores web 26 y 27 a través de Internet. Además, los ordenadores personales 29 pueden comunicarse con los servidores web 26 y 27 a través de Internet usando procedimientos de acceso a Internet convencionales, tales como los proporcionados por un proveedor de servicios de Internet. Dichas comunicaciones pueden enviarse usando el protocolo de transferencia de archivos (FTP), protocolo de transferencia de hipertexto (HTTP) y protocolo de transferencia de hipertexto sobre capas de conexión segura (HTTPS). La comunicación puede consistir en diversos tipos de archivos, incluyendo lenguaje de marcado de hipertexto (HTML), archivos de imagen y scripts del lado del cliente en lenguajes tal como JavaScript. Adicionalmente, tales mensajes pueden incluir archivos relacionados con diversos esquemas de seguridad, tales como certificados digitales y claves de firma. Adicionalmente, esta red ejemplar 10 incluye un servidor de autoridad de certificación (CA) 23 que es un servidor web que está configurado para actuar como una autoridad de certificación, incluyendo la capacidad de emitir certificados digitales y claves públicas y privadas para los servidores web tales como los servidores web 26 y 27 en esta red ejemplar. Además, el servidor CA 23 puede comunicarse con los terminales móviles 28 a través de la red móvil para mantener su conjunto de certificados raíz al día.

Con el fin de permitir a un script del lado del cliente acceder de forma segura a diversos recursos o datos en un ordenador, un terminal móvil 28 o un navegador web que funciona en un ordenador personal 29 puede programarse o configurarse para tomar ciertas medidas antes de ejecutar etapas que concederían al script acceso a dichos recursos o datos. Un resumen de un ejemplo de dichas medidas se ilustra en la figura FIG. 2, que muestra las etapas que pueden ejecutarse en un terminal móvil. El proceso puede desencadenarse cuando el script intenta acceder a un recurso, datos o procedimiento privilegiados, etapa 40. Un ejemplo de un procedimiento privilegiado incluye una solicitud para acceder a un historial de llamadas de un dispositivo móvil recibido desde un programa de correo electrónico basado en web, o un intento por parte de un programa de mapeo basado en web de acceder a las coordenadas GPS del dispositivo móvil. Antes de conceder acceso al recurso privilegiado, el navegador puede configurarse para verificar que el script particular que está intentando acceder al recurso es de confianza o de otro modo no es malicioso. Este procedimiento de resumen proporciona procedimientos alternativos para dicha verificación.

En primer lugar, el terminal móvil puede determinar si el intento de acceso se hace por un script que es absolutamente de confianza, prueba 42. Si un archivo es "de confianza" puede determinarse en varios procedimientos. Algunos de dichos procedimientos implican el uso de certificados digitales emitidos por autoridades de certificación, como se describe a continuación. Si el script es absolutamente de confianza (es decir, prueba 42 = "Sí"), el navegador puede ejecutar el script, etapa 44. Es útil para el código ser absolutamente de confianza, independientemente de la fuente directa del script, cuando el código no cambia con frecuencia. Por ejemplo, si un juego basado en web puede ser absolutamente de confianza el juego puede desarrollarse en cualquier ubicación y distribuirse a diversos sitios web después de designarse como de confianza. El juego puede entonces ser de confianza por el navegador de recepción incluso si el servidor en el que se aloja es desconocido para el terminal móvil o de otro modo sospechoso. La medida en que el script es fiable (es decir, si el juego puede acceder a un recurso, como una cámara o transferir un archivo del terminal móvil a un servidor remoto) puede determinarse en el momento en que el código se marca como fiable y se incluye dentro del certificado de confianza de manera que el dispositivo móvil pueda determinar a qué recursos particulares y procedimientos privilegiados puede acceder el script.

Si el script no es absolutamente fiable (es decir, prueba 42 = "No"), entonces el navegador puede determinar la confianza a través de un procedimiento alternativo. El navegador puede determinar si el servidor que proporcionó el código es de confianza, prueba 46 y si es así permitir el acceso, etapa 44. Si el servidor no es fiable (es decir, prueba 46 = "No"), entonces el navegador puede determinar que el script no es seguro y denegar el acceso al procedimiento protegido, etapa 50. Sin embargo, el navegador no siempre puede ejecutar un script solamente porque el servidor sea de confianza. En cambio, también puede verificar que el servidor es de confianza con respecto al procedimiento o recurso específico, prueba 48. Si el servidor no es de confianza para el procedimiento o recurso específico (es decir, prueba 48 = "No"), el navegador puede denegar el acceso al procedimiento, etapa 50. Si el servidor es de confianza para el procedimiento o recurso específico (es decir, etapa 48 = "Sí"), el navegador puede permitir el acceso al recurso, etapa 44.

El diagrama de flujo ilustrado en la FIG. 2 puede implementarse en realizaciones que determinan si se le puede conceder permiso a un script para obtener acceso a un recurso restringido en el momento en que se hace una solicitud para el acceso al recurso. Tal realización, que puede denominarse como un "tiempo de actuación" o durante la realización de ejecución, tiene diversas ventajas y desventajas. Una realización alternativa, que también tiene diversas ventajas y desventajas, es determinar qué recursos requerirá el script antes de ejecutarse el script. Para implementar tal "tiempo de carga" o antes de la realización de ejecución, el navegador web puede examinar los certificados digitales antes de la ejecución y generar una lista de recursos que pueden requerirse. En una realización alternativa, los scripts que requieren acceso a recursos potencialmente protegidos pueden indicar los recursos requeridos dentro de la sección de observaciones del script. En tal realización, la sección de observaciones del script puede leerse antes de la ejecución del script para determinar los recursos protegidos a los que se puede acceder. Una vez que el dispositivo móvil o el navegador web tiene la lista de recursos que necesitará un script, este puede realizar comprobaciones del estado de confianza del script y conjunto de permisos en un "lote" e impedir que el script se ejecute si requiere un recurso más allá de su conjunto de permisos.

Como se mencionó anteriormente, las diversas realizaciones permiten al navegador determinar si un sitio web es de confianza usando firmas digitales. Se muestra un resumen de cómo funcionan las firmas digitales en la FIG. 3A, que muestra etapas que pueden implementarse en instrucciones de software que se ejecutan en uno o más servidores 23, 26 y un ordenador personal o dispositivo móvil 28. Un servidor de autoridad de certificación (CA) 23 puede generar un par de claves de cifrado que un servidor web 26 puede usar para firmar digitalmente un documento, etapa 70. Como se conoce bien en las técnicas informáticas, las claves de cifrado son números enteros grandes que típicamente son números primos. Ciertos algoritmos de cifrado, tales como el RSA ya conocido, usan diferentes claves para el cifrado y el descifrado y juntos se conocen como un par de claves. Un par de clave pública/clave privada es un par de claves en el que la clave pública, que a menudo es la clave de descifrado, se publica o se incluye en documentos, mientras que la clave privada, que a menudo es la clave de cifrado, se mantiene en privado. Cualquier archivo o secuencia de datos informáticos que puede descifrarse con éxito por la clave pública debe haberse cifrado por la clave privada. Por lo tanto, si el servidor web 26 es la única entidad para conocer la clave privada, la identidad del servidor web 26 puede verificarse. Sin embargo, este procedimiento de verificación de identidad requiere que la clave pública sea verificable. Si una aplicación de cliente se equivoca en cuanto al valor de la clave pública, la aplicación puede engañarse al confiar en una entidad maliciosa. Un certificado digital es una herramienta que una aplicación de cliente puede usar para verificar la clave pública. El servidor CA 23 puede generar un certificado que contiene información tal como el nombre y la dirección URL del servidor web 26, así como la clave pública real del servidor web 26 y "firmar" el certificado cifrándolo con su propia clave privada (es decir, no la clave privada del servidor web 26), etapa 71.

El servidor web 26 comienza el proceso de firmar un documento, tal como un archivo JavaScript, calculando su huella, etapa 72, usando una técnica hash, tal como MD2. Una vez que la huella del documento se ha generado, el servidor web 26 puede "firmar" la huella cifrando la huella usando la clave privada como la clave de encriptación, etapa 74. Después el servidor web 27 puede transmitir el documento original junto con la huella firmada y el certificado digital al terminal móvil 28, etapa 76.

Los documentos se reciben por el terminal móvil 28, etapa 77 y el terminal móvil 28 puede determinar la clave pública del servidor CA 23 de su conjunto raíz almacenado en la memoria. Como se ha descrito anteriormente, el conjunto raíz es un conjunto de certificados en los que el terminal móvil 28 puede confiar inherentemente (es decir, el terminal móvil 28 puede asumir que todos los certificados en su conjunto raíz son auténticos). Usando la clave pública del servidor CA 23 como la clave de desencriptación, el terminal móvil puede descifrar el certificado digital para verificar la clave pública del servidor web 26, etapa 79. Con la clave pública del servidor web 26 como la clave de descifrado, el terminal móvil 28 puede descifrar la huella firmada para descubrir la huella original, etapa 80. El terminal móvil también puede calcular la huella del documento usando la misma técnica hash (por ejemplo, MD2), etapa 82. Después el terminal móvil puede comparar las dos huellas para comprobar la igualdad, etapa 84. Si la huella calculada por el terminal móvil equivale a la huella descifrada, entonces el dispositivo móvil ha confirmado que el documento procede de una fuente de confianza por el servidor CA 23 y que el documento no se ha alterado desde que dejó el control del servidor web 26. Por lo tanto, si las huellas de documento calculadas y descifradas son iguales, prueba 86, el documento es de confianza, pero si no es así, el documento no es de confianza.

Puede haber un beneficio comercial y/o técnico en el "encadenamiento de confianza" o permitir que los certificados se emitan por fuentes distintas de una autoridad de certificación inherentemente de confianza ("autoridad principal"). En una situación tal los terminales móviles bien necesitarían confiar en la nueva autoridad de certificación inherentemente añadiendo el certificado de la nueva autoridad de certificación al conjunto raíz, o bien realizar algunas etapas para verificar que la nueva autoridad de certificación es de confianza para la autoridad principal. Un ejemplo de un procedimiento que realiza esta tarea se ilustra en la FIG. 3B, que muestra etapas que pueden ejecutarse en un terminal móvil o un ordenador personal.

Un terminal móvil que está intentando verificar la fiabilidad de un certificado presentado puede comenzar examinando el certificado para determinar si el certificado está firmado por una autoridad principal, prueba 54. El certificado presentado corresponderá típicamente a un protocolo estándar, tal como el ya conocido ITU-T X.509, que incluye datos en relación con la identidad de la autoridad firmante. El terminal móvil puede comparar la identidad de la autoridad firmante con el conjunto de certificados en el conjunto raíz. Si hay una correspondencia (es decir, prueba 54 = "Sí"), entonces el terminal móvil puede asumir que el certificado presentado es fiable, etapa 56. Si el terminal móvil no reconoce el certificado actual como uno firmado por una autoridad principal, puede determinar si el certificado se firmó por otro servidor (en vez de autofirmarse como algunos certificados raíz están), prueba 58. Si el certificado actual no se firmó por otra autoridad (es decir, prueba 58 = "No"), entonces el terminal móvil puede determinar que el certificado no es fiable, etapa 60. Sin embargo, si el certificado actual se firmó por otra autoridad (es decir, prueba 58 = "Sí"), el terminal móvil puede entonces recuperar el certificado de esa autoridad, etapa 64. La cadena de certificados puede presentarse toda al mismo tiempo, o puede recuperarse de la autoridad de certificación a petición según se establece en el certificado. Una vez que el terminal móvil ha localizado el nuevo certificado (es decir, etapa 64), este puede determinar si ese certificado es de confianza repitiendo etapas similares para el nuevo certificado. En la mayor parte de los casos, el terminal móvil determinará finalmente qué certificados están encadenados a partir de una autoridad inherentemente de confianza y cuáles no.

Diversas realizaciones pueden emplear un sistema de permisos para que la fiabilidad sea más precisa. Por ejemplo, puede no ser ideal permitir un acceso completo del sitio web a un terminal móvil, aunque pueda ser de confianza para algunos usos. Como alternativa, algunas autoridades de certificación pueden ser competentes para otorgar fiabilidad a algunos recursos pero no otros. Este tipo de información puede incrustarse en los certificados digitales emitidos por las autoridades de certificación. Se conoce bien en la técnica que los certificados digitales incluyen información tal como la dirección URL del sitio web y el nombre de la entidad a la que la dirección URL está registrada. De hecho, los certificados digitales pueden soportar cualquier tipo de datos legibles por ordenador, sean binarios, de texto o cualesquiera otros. En algunas realizaciones, las autoridades de certificación pueden usar una serie de identificadores únicos en un espacio de nombres bien definidos para comunicar permisos. Dichos permisos enumerados pueden incluir una lista de recursos o categorías de recursos para terminal móvil para los que se le ha concedido permiso al servidor para acceder. Por ejemplo, un navegador web puede conceder a un sitio web acceso a las coordenadas geográficas del terminal móvil únicamente cuando cada certificado en la cadena de confianza incluye la frase explícita "conceder coordenadas geográficas" o un código o símbolo digital equivalente. También es posible para las autoridades de certificación emitir certificados que sean válidos para firmar documentos, pero no para emitir otro certificado, lo que tiene el efecto de limitar el número de posibles enlaces en la cadena de confianza. En una realización tal, un navegador web puede determinar si se le ha concedido permiso al servidor para acceder a un recurso solicitado basándose en el certificado digital emitido al servidor, tal como leyendo la lista de permisos incluida en el certificado. Por lo tanto, un navegador web o dispositivo móvil puede no confiar en un certificado que se firma por una entidad cuyo certificado carece de la frase "conceder autoridad de certificación" o un código o símbolo digital equivalente.

Además de los esquemas de permiso que incorporan los certificados digitales, los usuarios pueden conceder explícitamente ciertos permisos a los sitios web. Por ejemplo, un usuario puede desear ejecutar una aplicación web que requiere acceso a un recurso para el que el sitio web no se ha certificado por una autoridad de confianza. Este sitio web puede ser un sitio web comercial bien conocido que tiene acuerdos mercantiles que lo impiden colaborar con cualquiera de las autoridades principales o sus derivados. Como alternativa, puede ser un sitio web que el usuario desarrolló personalmente. El usuario puede conceder expresamente recursos o grupos de recursos a los

sitios web basándose en la URL. Aunque esta opción puede tener desventajas desde una perspectiva de seguridad, también puede tener ventajas comerciales que superan las desventajas, especialmente para los usuarios entendidos.

En una realización adicional, el propio script, o los datos adjuntos al script, puede incluir información que limita los permisos concedidos al script. En esta realización, el script, o los datos adjuntos al script pueden limitar el acceso a los recursos menos que aquellos a los que se le ha concedido permiso al servidor para acceder al certificado digital emitido al servidor.

Utilizando algunas de las técnicas de seguridad que se han mencionado anteriormente, un entorno de navegación web puede hacerse seguro. Las comunicaciones que permiten tal entorno se ilustran en la FIG. 4A, que es un diagrama de tiempos que muestra ciertas comunicaciones, que pueden producirse entre diversos sistemas. Con el fin de facilitar la cadena de confianza, un servidor CA 23 puede enviar el conjunto raíz de certificados al terminal móvil 28, mensajes 105. Esta comunicación de certificados del conjunto raíz puede transmitirse en cualquier momento y típicamente se actualiza periódicamente como parte de los servicios normales proporcionados a los dispositivos móviles. El servidor CA 23 también puede crear un certificado y el par de claves para enviar al servidor web 26, mensajes 110. Con estas herramientas de seguridad idóneas, el terminal móvil 28 puede navegar opcionalmente a un sitio web alojado por el servidor web 26 y abrir una conexión segura entre el dispositivo y el servidor, mensajes opcionales 115. Como alternativa, el terminal móvil 28 puede usar una conexión segura, tal como seguridad de la capa de transporte (TLS), o simplemente contar con la infraestructura del sistema de nombres de dominio (DNS) para comunicar con el servidor 26. Después el terminal móvil 28 puede solicitar una página web del servidor web 26, mensaje 120. El servidor web 26 puede responder a la solicitud con un código firmado para que el terminal móvil 28 lo ejecute, mensaje 125. El código puede estar firmado por el servidor web 26 de manera similar al procedimiento de firma digital que se ha descrito anteriormente con referencia a la FIG. 3A, o el código puede enviarse al servidor CA 23 a través de una solicitud HTTP donde puede firmarse por el servidor CA 23 y devolverse al servidor web 26 a través de una respuesta HTTP. Este proceso puede repetirse una o más veces según el usuario del terminal móvil 28 continúa navegando por el sitio web, mensajes 120 y 125. Si el terminal móvil 28 verifica la firma digital proporcionada con el código (como se ha descrito anteriormente con referencia a la FIG. 3A), el terminal móvil 28 puede proporcionar al script acceso a un recurso, datos o un procedimiento privilegiados que después puede transmitir algunos o todos estos datos confidenciales al servidor 26, mensaje 127. Usando dichos datos confidenciales, el servidor 26 puede entonces proporcionar a una página web, datos o el script en los que se basa, en respuesta a o de otro modo específicos a la información confidencial, mensaje 129. Por ejemplo, si los datos solicitados proporcionados al servidor 26 en el mensaje 127 son las coordenadas GPS del dispositivo móvil 28, el servidor 26 puede proporcionar una página web que sea específica a la ubicación del dispositivo, tal como un mapa local o números de teléfonos de negocios cercanos.

En una realización alternativa, un dispositivo móvil 28 puede solicitar y recibir una firma digital de una autoridad firmante aparte de recibir una página web de otro servidor. Esta realización se ilustra en las FIG. 3C y 4B. Haciendo referencia a la FIG. 3C, el proceso procede similar al que se ha descrito anteriormente con referencia a la FIG. 3A con la adición del dispositivo móvil que envía una solicitud http separada a la autoridad firmante 23 o el servidor del proveedor de la aplicación web original que envía una firma digital para la página web y recibiendo la firma en respuesta, etapa 78. En la autoridad firmante 23, se recibe la solicitud de una firma digital, etapa 88 y en respuesta, la autoridad firmante 23 devuelve una firma digital que puede almacenarse en la memoria del servidor, etapa 89. Esta etapa adicional se ilustra en el diagrama de flujo de mensajes mostrado en la FIG. 4B como una solicitud de firma a la autoridad firmante, mensaje 130, seguida de la transmisión de la firma de vuelta al dispositivo móvil, mensaje 132.

Una ilustración más detallada de cómo un terminal móvil y un servidor web pueden interactuar se muestra en la FIG. 5, que muestra etapas que pueden implementarse en instrucciones de software ejecutadas en el servidor 26 y un dispositivo móvil 28 o un ordenador personal. El usuario del terminal móvil 28 puede solicitar una página web del servidor web 26, etapa 136. Esta solicitud puede transmitirse usando procedimientos de red de datos móviles ya conocidos y a través de Internet. En respuesta, el servidor web 26 puede generar un código de una manera conocida usando un intérprete PHP, etapa 138. El servidor web 26 puede firmar este código generado dinámicamente, etapa 140, usando procedimientos descritos más detalladamente antes con referencia a la FIG. 3A. Después el servidor web puede transmitir el código firmado de vuelta al dispositivo móvil, tal como usando procedimientos conocidos de red de datos móviles e Internet. Una vez que el dispositivo recibe el código firmado, puede comenzar a ejecutar el código, etapa 145. Cuando el código solicita acceso a un recurso restringido tal como un determinado archivo, etapa 150, el terminal móvil 28 puede pausar la ejecución del script para verificar si el código es fiable para acceder a ese recurso, etapa 155. Esta verificación se realiza usando los procedimientos que se han descrito anteriormente con referencia a la FIG. 3A. Si el terminal móvil determina que el código es fiable puede conceder el acceso, etapa 157.

En una realización alternativa, un certificado digital para el servidor puede configurarse previamente en el cliente (es decir, el dispositivo móvil), igual que lo están las claves raíz. Por lo tanto, en esta realización, la etapa de recibir un certificado digital descrita anteriormente es opcional ya que el certificado digital ya puede estar disponible en la memoria del terminal móvil. En dichas situaciones, el proceso para verificar y ejecutar una aplicación implica que el dispositivo móvil reciba un script para su ejecución desde el servidor, que el dispositivo móvil verifique que el

servidor del que se obtuvo el script está nombrado en un certificado digital (que ya puede estar en la memoria o puede proporcionarse por separado), que el dispositivo móvil determine qué permisos se han concedido al servidor de acuerdo con el contenido del certificado y que el dispositivo móvil permita al script acceder a un recurso protegido únicamente cuando se ha concedido un permiso asociado al servidor del que se obtuvo el script.

Los entornos de navegación web que no utilizan las fuertes medidas de seguridad descritas en el presente documento pueden escoger limitar la funcionalidad del script prohibiendo a los scripts que se integren con scripts que proceden de servidores distintos del servidor particular del que se originó el script. Por ejemplo, una página web puede incluir un script JavaScript para generar un sistema de menús. Puede ser útil para un sistema de menús de un sitio web tener enlaces a nuevos sitios web o sitios web de información meteorológica. Sin embargo, los navegadores web tal como Firefox® e Internet Explorer® pueden no permitir al script del menú que se comunique con el servidor de noticias. En un entorno de navegación de confianza, tal prohibición puede levantarse fácilmente. Un ejemplo de un terminal móvil que permite a un script ponerse en contacto con un segundo servidor se muestra en la FIG. 6, que muestra las comunicaciones que pueden producirse entre los sistemas. El terminal móvil 28 puede navegar por un sitio web en el servidor web 26 y los sistemas pueden establecer una conexión segura, mensajes 115. El terminal móvil 28 puede solicitar una página web del servidor web 26, mensaje 120. El servidor web 26 puede responder a la solicitud con un código firmado para que el terminal móvil 28 lo ejecute, mensaje 125. En respuesta a la ejecución del código del servidor web 26, el terminal móvil puede solicitar un script de otro servidor web 27 para extender la funcionalidad del script de menú actual, mensaje 121. El servidor web 27 genera un código y lo firma y envía el código firmado al terminal móvil 28, mensaje 126. En un navegador web tradicional, el navegador web puede impedir la ejecución del script desde el navegador web, o limita su capacidad de interactuar con el documento existente.

Las realizaciones que se han descrito anteriormente pueden implementarse en cualesquiera de una diversidad de terminales móviles, tales como, por ejemplo, teléfonos móviles, asistentes personales de datos (PDA) con teléfono móvil, receptores de correo electrónico móviles, dispositivos de acceso web móviles y otros dispositivos equipados con procesador que puedan desarrollarse en el futuro que se conecten a una red inalámbrica. Típicamente, dichos terminales móviles tendrán en común los componentes ilustrados en la FIG. 7. Por ejemplo, el terminal móvil 170 puede incluir un procesador 171 acoplado a la memoria interna 172 y una pantalla 173. Adicionalmente, el terminal móvil 170 tendrá una antena 174 para enviar y recibir radiación electromagnética que se conecta a un enlace de datos inalámbrico y/o un transceptor de telefonía móvil 175 acoplado al procesador 171. En algunas implementaciones, el transceptor 175 y las porciones del procesador 171 y la memoria 172 usadas para las comunicaciones de telefonía móvil se denominan como la interfaz aérea ya que proporcionan una interfaz de datos a través de un enlace de datos inalámbrico.

El procesador 171 puede ser cualquier microprocesador programable, microordenador o un chip o chips de procesador múltiple que pueden configurarse mediante instrucciones de software (aplicaciones) para realizar una diversidad de funciones, incluyendo las funciones de las diversas realizaciones que se han descrito anteriormente. En algunos terminales móviles, pueden proporcionarse múltiples procesadores 171, tales como un procesador dedicado a funciones de comunicación inalámbrica y un procesador dedicado a la ejecución de otras aplicaciones. Típicamente, las aplicaciones de software pueden almacenarse en la memoria interna 172 antes de accederse y cargarse en el procesador 171. En algunos terminales móviles, el procesador puede incluir memoria interna suficiente para almacenar las instrucciones del software de aplicación. Para los fines de esta descripción, el término memoria se refiere a toda memoria accesible por el procesador 171, incluyendo memoria interna 172 y memoria en el propio procesador 171. Los archivos de datos del usuario se almacenan típicamente en la memoria 172. En muchos terminales móviles, la memoria 172 puede ser una memoria volátil o no volátil, tal como una memoria flash, o una mezcla de ambas. Típicamente, los terminales móviles incluirán un teclado 176 o un teclado en miniatura y botones o interruptores de selección de menú 177 para recibir las entradas de usuario.

Las realizaciones que se han descrito anteriormente también pueden implementarse en cualesquiera de una diversidad de dispositivos de computación, tales como, por ejemplo, un ordenador personal 29 ilustrado en la FIG. 8. Tal ordenador personal 29 incluye típicamente una carcasa del ordenador 160, un procesador 161 acoplado a la memoria volátil 162 y una memoria no volátil de gran capacidad, tal como un disco duro 163. El ordenador 29 también puede incluir una unidad de disco flexible 164 y una unidad de disco compacto (CD) 165 acopladas al procesador 161. Típicamente el ordenador 29 también incluirá un dispositivo de entrada de usuario como un teclado 166 y una pantalla 137. El ordenador 29 también puede incluir varios puertos conectores para recibir dispositivos de memoria externos acoplados al procesador 161, tales como un puerto bus serie universal (USB) (no mostrado), así como circuitos de conexión de red (no mostrados) para acoplar el procesador 161 a una red. En una configuración portátil, la carcasa del ordenador 160 incluye el teclado 166 y la pantalla 137.

En una o más realizaciones a modo de ejemplo, las funciones descritas pueden implementarse en hardware, software, firmware o en cualquier combinación de los mismos. Si se implementan en software, las funciones pueden almacenarse en o transmitirse como una o más instrucciones o código en un medio legible por ordenador. Los medios legibles por ordenador incluyen tanto medios de almacenamiento informáticos como medios de comunicación, incluyendo cualquier medio que facilite la transferencia de un programa informático de un lugar a otro. Los medios de almacenamiento pueden ser cualesquiera medios disponibles a los que pueda accederse mediante

un ordenador. A modo de ejemplo y no de manera limitativa, tales medios legibles por ordenador pueden comprender RAM, ROM, EEPROM, CD-ROM u otro almacenamiento de disco óptico, almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para transportar o almacenar código de programa deseado en forma de instrucciones o estructuras de datos y al que pueda accederse mediante un ordenador. Además, cualquier conexión puede denominarse de manera apropiada medio legible por ordenador. Por ejemplo, si el software se transmite desde un sitio web, un servidor u otra fuente remota usando un cable coaxial, un cable de fibra óptica, un par trenzado, una línea de abonado digital (DSL) o tecnologías inalámbricas tales como infrarrojos, radio y microondas, entonces el cable coaxial, el cable de fibra óptica, el par trenzado, la DSL o las tecnologías inalámbricas tales como infrarrojos, radio y microondas se incluyen en la definición de medio. Los discos, tal y como se usan en el presente documento, incluyen discos compactos (CD), discos de láser, discos ópticos, discos versátiles digitales (DVD), discos flexibles y discos blu-ray, donde los discos normalmente reproducen datos de manera magnética, así como de manera óptica con láseres. Las combinaciones de lo anterior también deben incluirse dentro del alcance de los medios legibles por ordenador.

REIVINDICACIONES

1. Un procedimiento para ejecutar una aplicación cliente-servidor en un dispositivo móvil, que comprende:

recibir de un servidor un script para su ejecución en el dispositivo móvil;

recibir un certificado digital emitido al servidor; verificar el certificado digital y confirmar que el script no se ha modificado desde que se creó el certificado digital;

determinar si se le ha concedido permiso al servidor para acceder a un recurso solicitado basándose en el certificado digital emitido al servidor;

permitir que el script acceda al recurso identificado en el certificado digital usado para verificar el script únicamente si se le ha concedido permiso al servidor para acceder al recurso solicitado; y transmitir algunos o todos los datos confidenciales relacionados con el recurso identificado al servidor.

2. El procedimiento de la reivindicación 1, que comprende adicionalmente recibir una firma digital para el script que comprende una primera huella encriptada del script,
en el que la etapa de verificar el certificado digital y confirmar que el script no se ha modificado comprende:

determinar que el certificado digital se emitió al servidor por un tercero de confianza;
determinar una clave pública del servidor a partir del certificado digital;

descifrar la huella encriptada usando una clave pública del servidor;

generar una segunda huella del script; y comparar el valor de la primera huella con el valor de la segunda huella.

3. El procedimiento de la reivindicación 1, que comprende adicionalmente determinar si se le debe conceder permiso al script acceder al recurso verificando a partir del certificado digital que un tercero de confianza ha concedido al servidor acceso al recurso o a una clase de recursos que contienen el recurso.

4. El procedimiento de la reivindicación 1, que comprende adicionalmente solicitar un servicio del servidor, en el que el script recibido se generó en el servidor en respuesta a la solicitud del servicio.

5. El procedimiento de la reivindicación 2, en el que determinar que el certificado digital se emitió al servidor por un tercero de confianza comprende determinar que el certificado digital se emitió al servidor por una autoridad de certificación que es inherentemente de confianza.

6. El procedimiento de la reivindicación 2, en el que determinar que el certificado digital se emitió al servidor por un tercero de confianza comprende determinar que el certificado digital se emitió al servidor por una autoridad de certificación que está vinculada a una autoridad de certificación inherentemente de confianza mediante una cadena de certificados digitales.

7. El procedimiento de la reivindicación 1, que comprende además:

solicitar una firma digital para el script del servidor; y

recibir una firma digital para el script en respuesta a la solicitud para la firma digital.

8. El procedimiento de la reivindicación 1, que comprende además:

limitar los permisos concedidos al script basándose en la información en el script; y

permitir al script acceder al recurso solicitado únicamente si el recurso solicitado se incluye en los permisos limitados.

9. Un programa informático que comprende instrucciones para realizar un procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 8.

10. Un dispositivo móvil, que comprende:

medios para recibir de un servidor un script para su ejecución en el dispositivo móvil
medios para recibir un certificado digital emitido al servidor;

medios para verificar el certificado digital y confirmar que el script no se ha modificado desde que se

creó el certificado digital;

medios para determinar si se le ha concedido permiso al servidor para acceder a un recurso solicitado basándose en el certificado digital emitido al servidor; y

medios para permitir que el script acceda al recurso únicamente si el certificado digital se verifica y el script no se ha modificado y si se le ha concedido permiso al servidor para acceder al recurso solicitado; y

medios para transmitir algunos o todos los datos confidenciales relacionados con el recurso identificado al servidor.

11. El dispositivo móvil de la reivindicación 10, que comprende adicionalmente medios para recibir una firma digital para el script en forma de una primera huella encriptada del script; y
en el que el medio para verificar el certificado digital y confirmar que el script no se ha modificado comprende:

medios para determinar que el certificado digital se emitió al servidor por un tercero de confianza;

medios para determinar una clave pública del servidor a partir del certificado digital;

medios para descifrar la huella encriptada usando una clave pública del servidor;

medios para generar una segunda huella del script; y

medios para comparar el valor de la primera huella con el valor de la segunda huella.

12. El dispositivo móvil de la reivindicación 10, que comprende adicionalmente medios para determinar si se le debe conceder permiso al script acceder al recurso verificando a partir del certificado digital que un tercero de confianza ha concedido al servidor acceso al recurso o a una clase de recursos que contienen el recurso.

13. El dispositivo móvil de la reivindicación 12, en el que el medio para determinar que el certificado digital se emitió al servidor por un tercero de confianza comprende medios para determinar que el certificado digital se emitió al servidor por una autoridad de certificación que es inherentemente de confianza.

14. El dispositivo móvil de la reivindicación 12, en el que el medio para determinar que el certificado digital se emitió al servidor por un tercero de confianza comprende medios para determinar que el certificado digital se emitió al servidor por una autoridad de certificación que se vincula a una autoridad de certificación inherentemente de confianza mediante una cadena de certificados digitales.

15. El dispositivo móvil de la reivindicación 11, que comprende adicionalmente:

medios para limitar los permisos concedidos al script basándose en la información en el script; y

medios para permitir al script el acceso al recurso solicitado solo si el recurso solicitado se incluye en los permisos limitados.

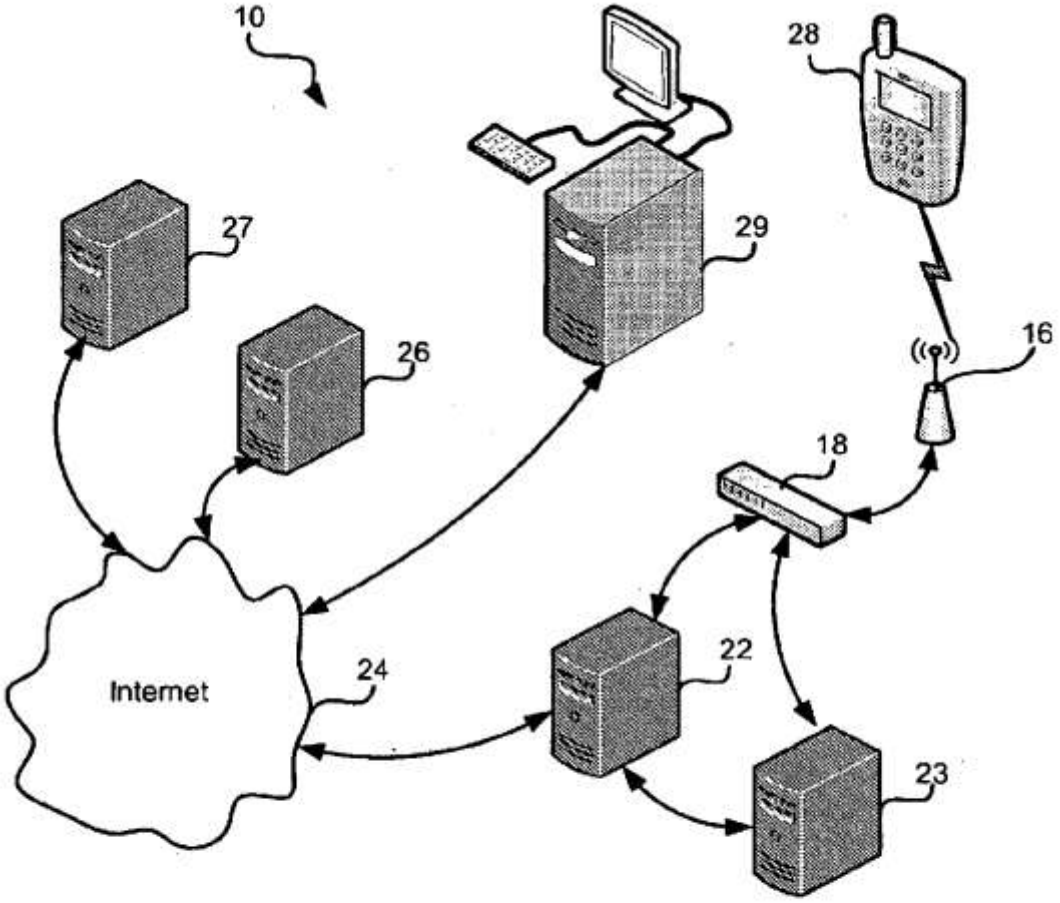

FIG. 1

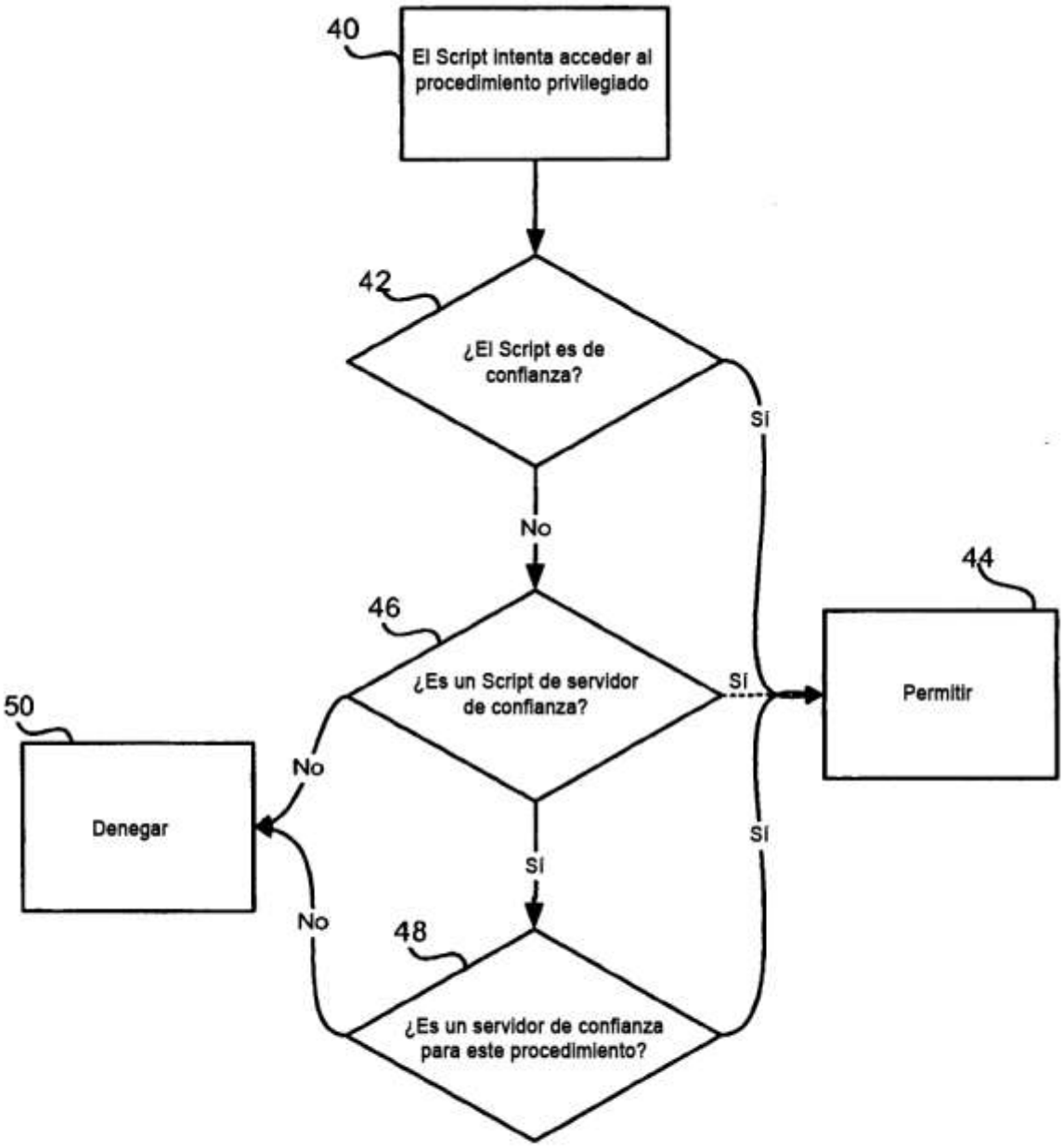
40
El Script intenta acceder al procedimiento privilegiado
42
¿El Script es de confianza?
Sí
No
44
46
¿Es un Script de servidor de confianza?
Sí
Permitir
50
No
Denegar
Sí
Sí
No
48
¿Es un servidor de confianza para este procedimiento?

FIG. 2

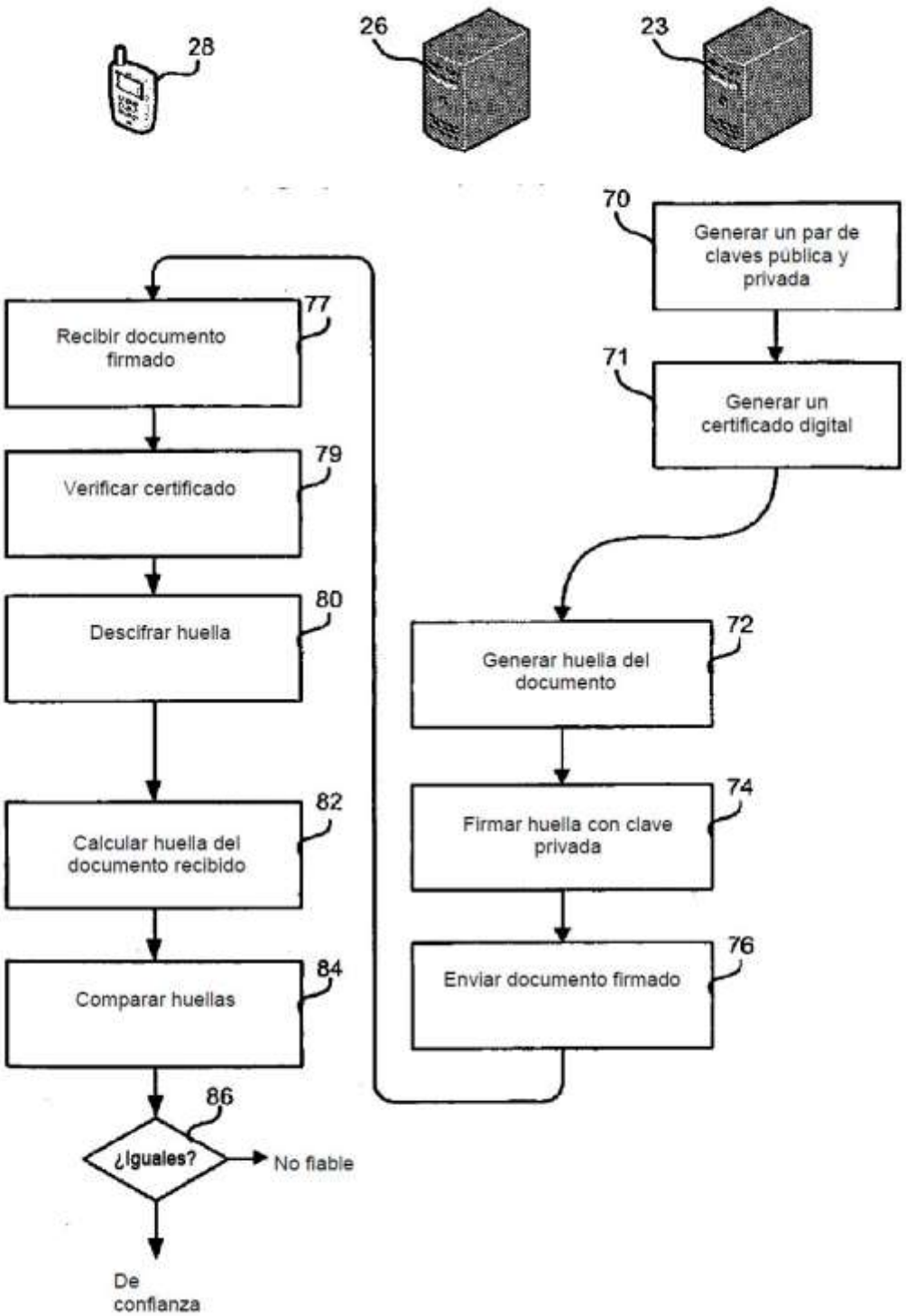
28
26
23
70
Generar un par de claves pública y privada
71
Generar un certificado digital
72
Generar huella del documento
74
Firmar huella con clave privada
76
Enviar documento firmado
77
Recibir documento firmado
79
Verificar certificado
80
Descifrar huella
82
Calcular huella del documento recibido
84
Comparar huellas
86
¿Iguales?
No fiable
De confianza

FIG. 3A

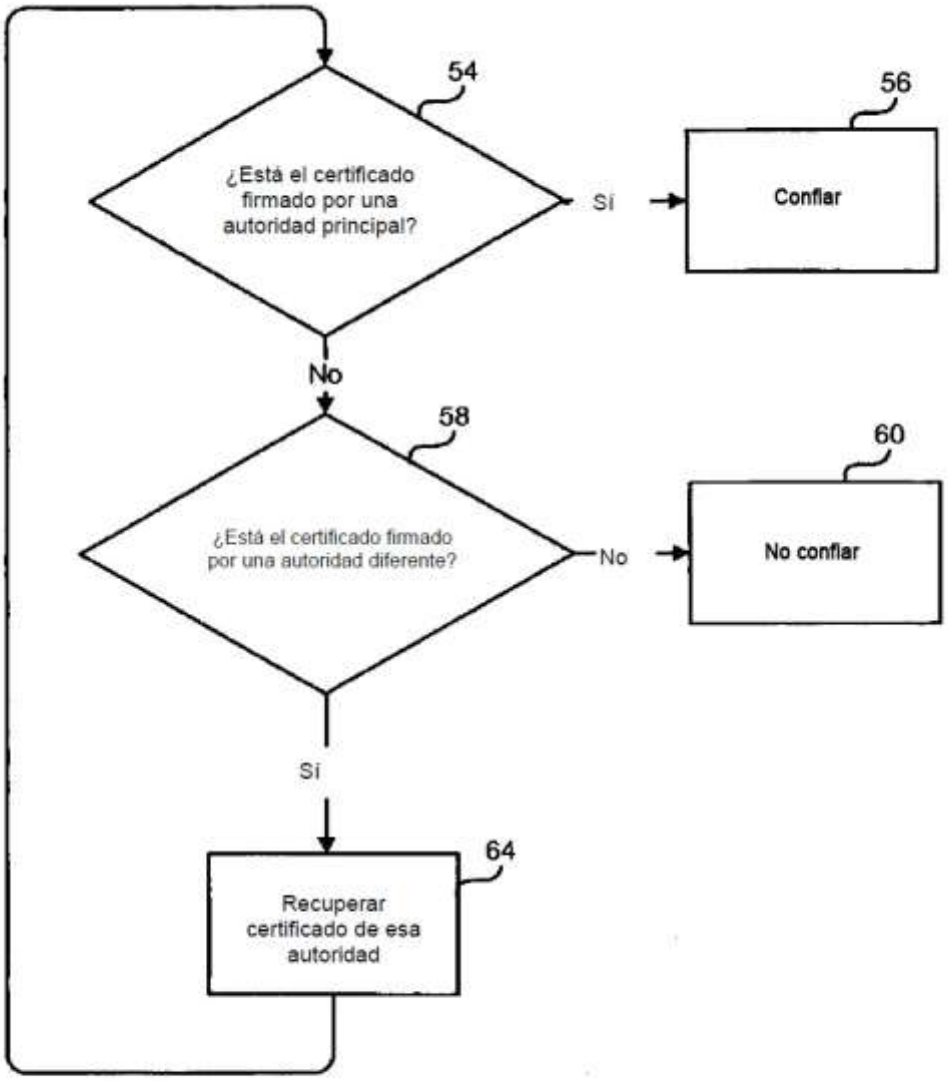
54
¿Está el certificado firmado por una autoridad principal?
Sí
56
Confiar
No
58
¿Está el certificado firmado por una autoridad diferente?
No
60
No confiar
Sí
64
Recuperar certificado de esa autoridad

FIG. 3B

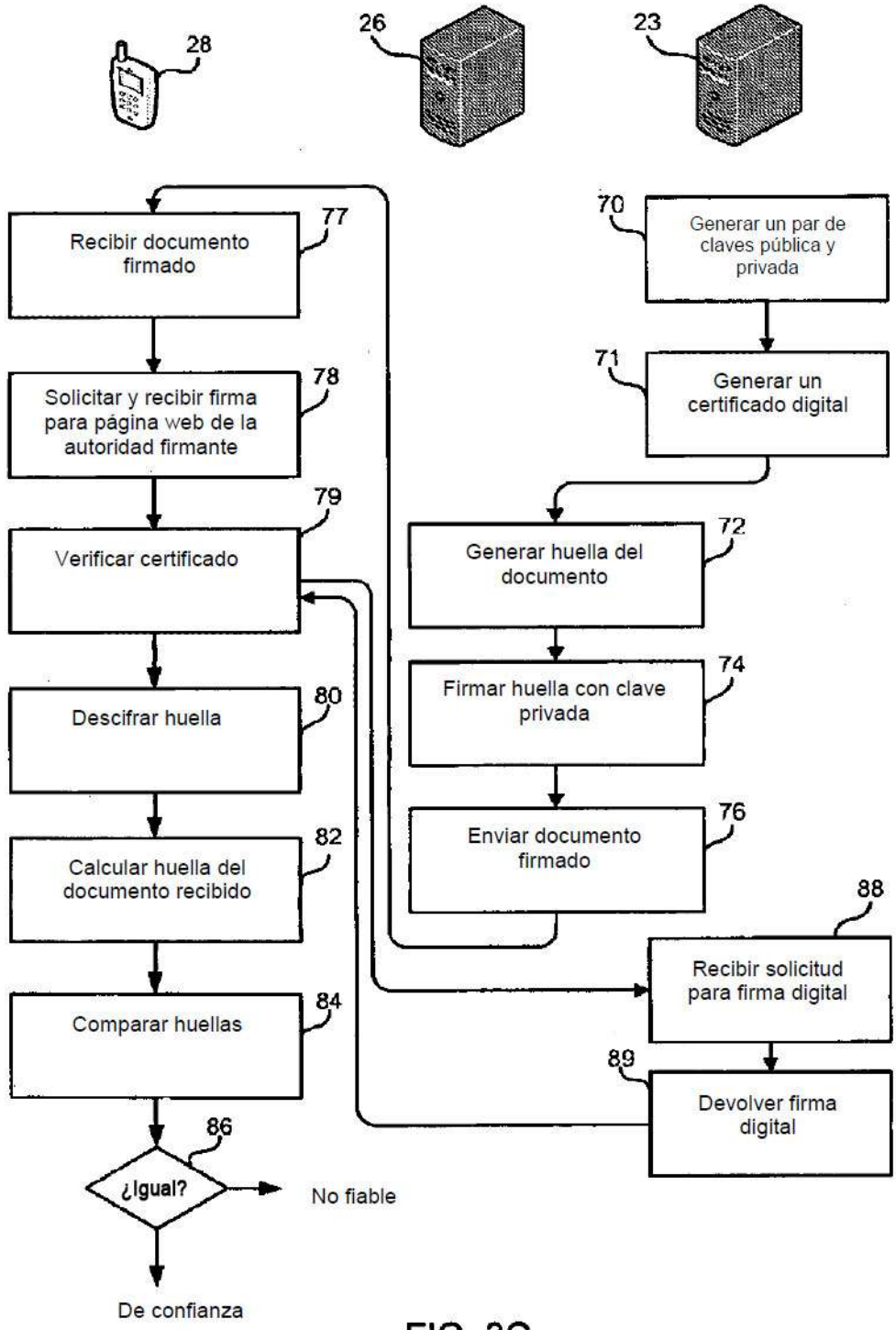
28
26
23
Recibir documento firmado
77
Solicitar y recibir firma para página web de la autoridad firmante
78
Verificar certificado
79
Descifrar huella
80
Calcular huella del documento recibido
82
Comparar huellas
84
¿Igual?
86
No fiable
De confianza
70
Generar un par de claves pública y privada
71
Generar un certificado digital
Generar huella del documento
72
Firmar huella con clave privada
74
Enviar documento firmado
76
88
Recibir solicitud para firma digital
89
Devolver firma digital

FIG. 3C

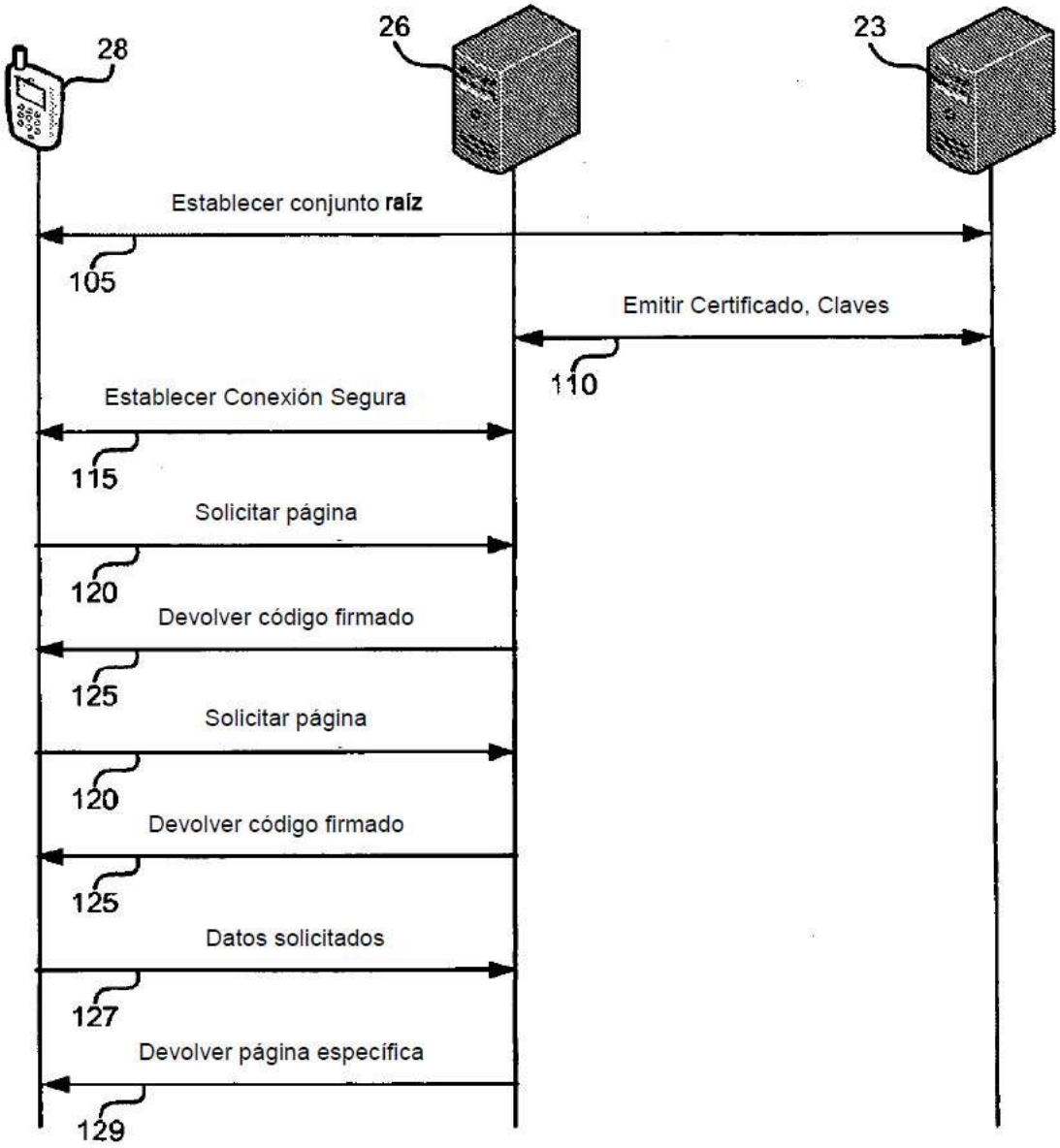
28
26
23
Establecer conjunto raíz
105
Emitir Certificado, Claves
110
Establecer Conexión Segura
115
Solicitar página
120
Devolver código firmado
125
Solicitar página
120
Devolver código firmado
125
Datos solicitados
127
Devolver página específica
129

FIG. 4A

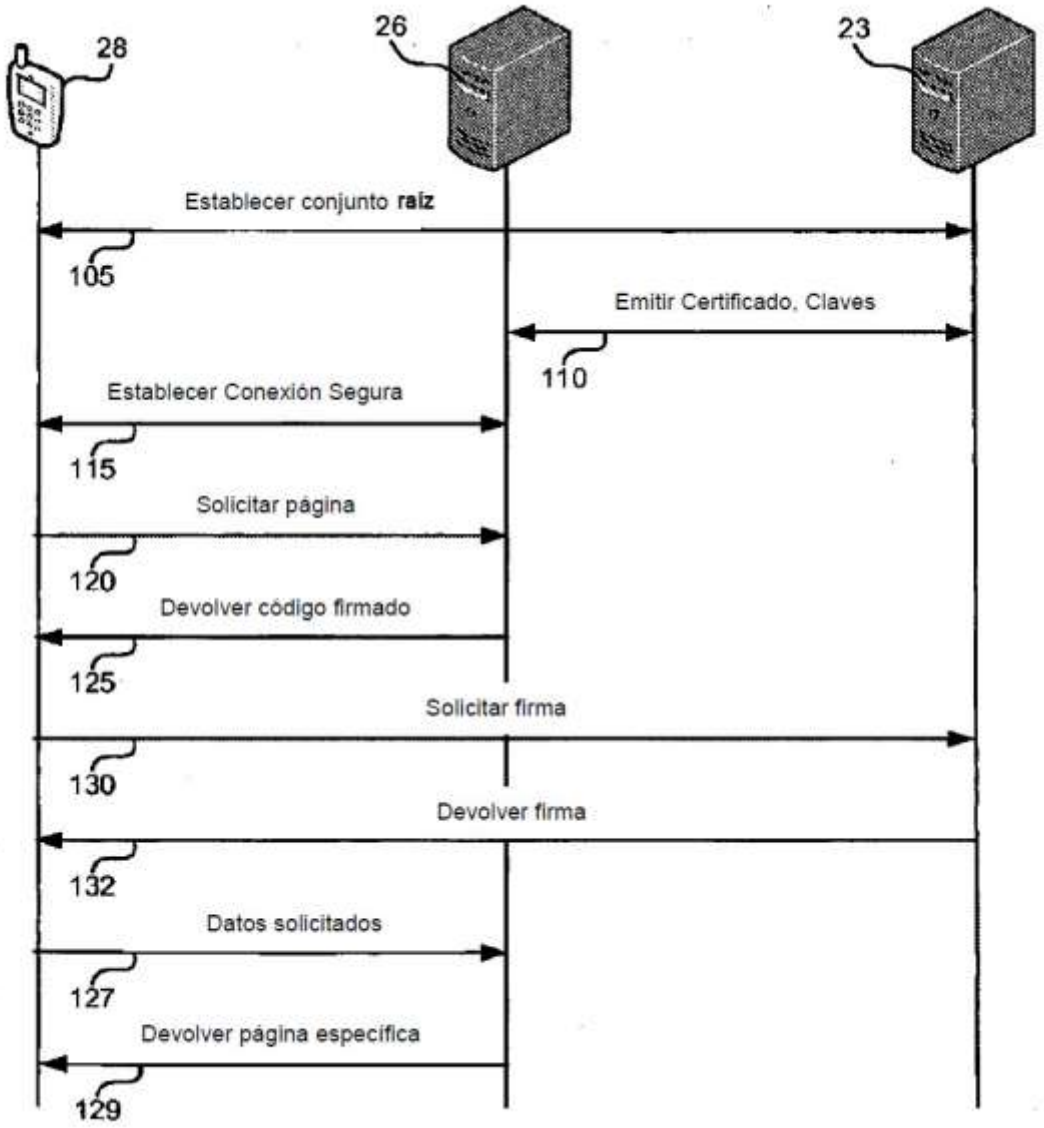
28
26
23
Establecer conjunto raíz
105
Emitir Certificado, Claves
110
Establecer Conexión Segura
115
Solicitar página
120
Devolver código firmado
125
Solicitar firma
130
Devolver firma
132
Datos solicitados
127
Devolver página específica
129

FIG. 4B

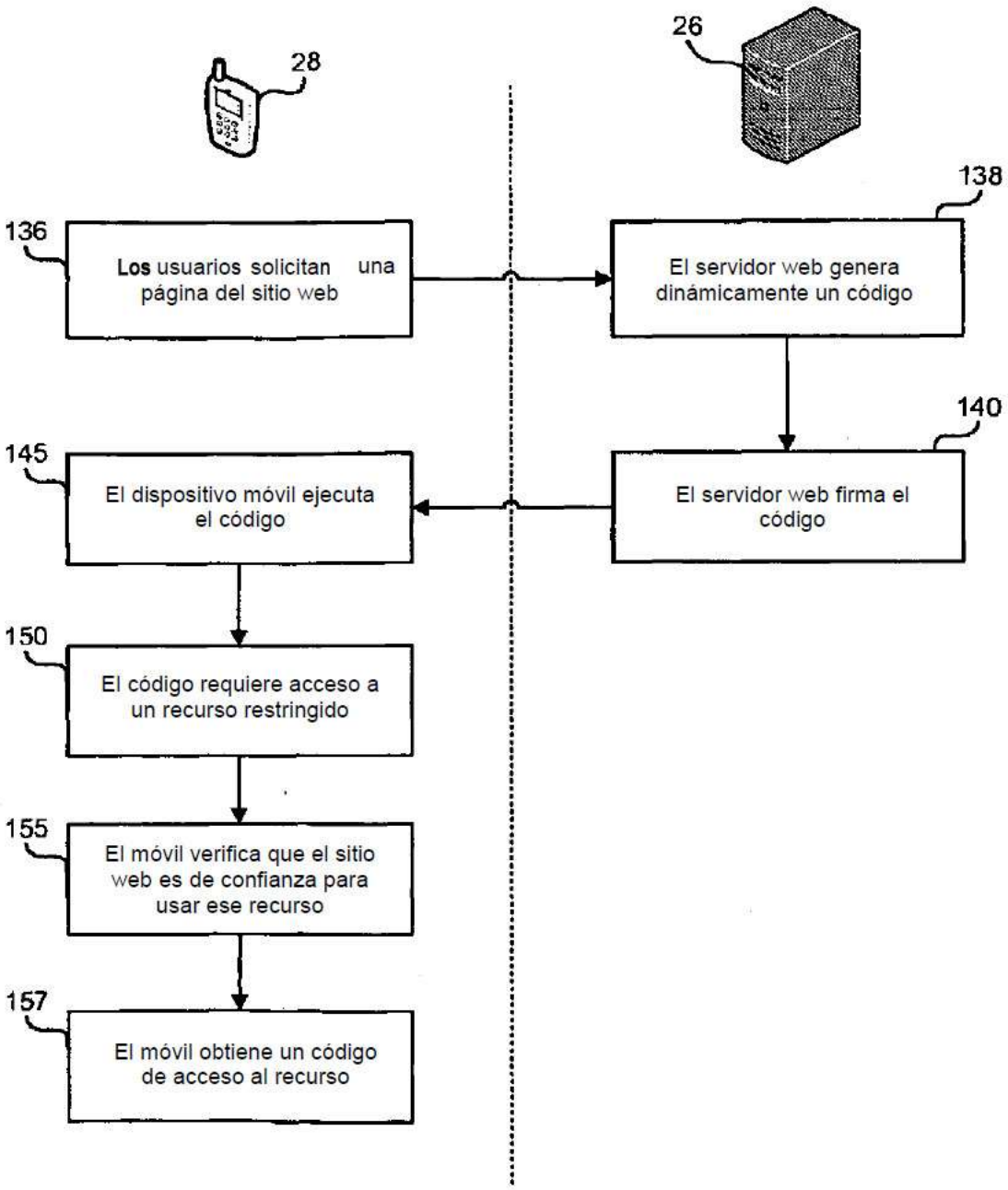
28
26
136
Los usuarios solicitan una página del sitio web
138
El servidor web genera dinámicamente un código
140
El servidor web firma el código
145
El dispositivo móvil ejecuta el código
150
El código requiere acceso a un recurso restringido
155
El móvil verifica que el sitio web es de confianza para usar ese recurso
157
El móvil obtiene un código de acceso al recurso

FIG. 5

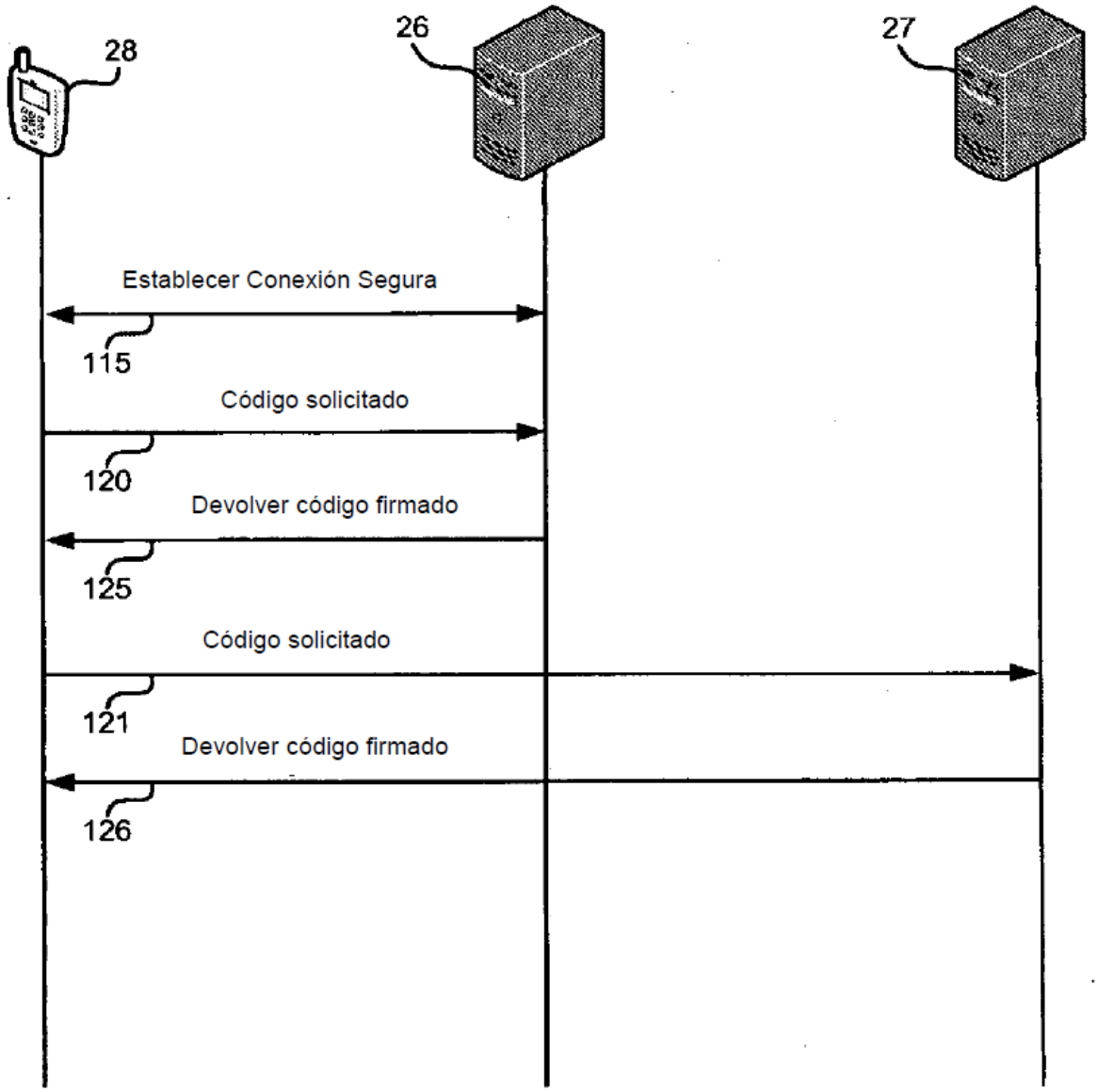
28
26
27
Establecer Conexión Segura
115
Código solicitado
120
Devolver código firmado
125
Código solicitado
121
Devolver código firmado
126

FIG. 6

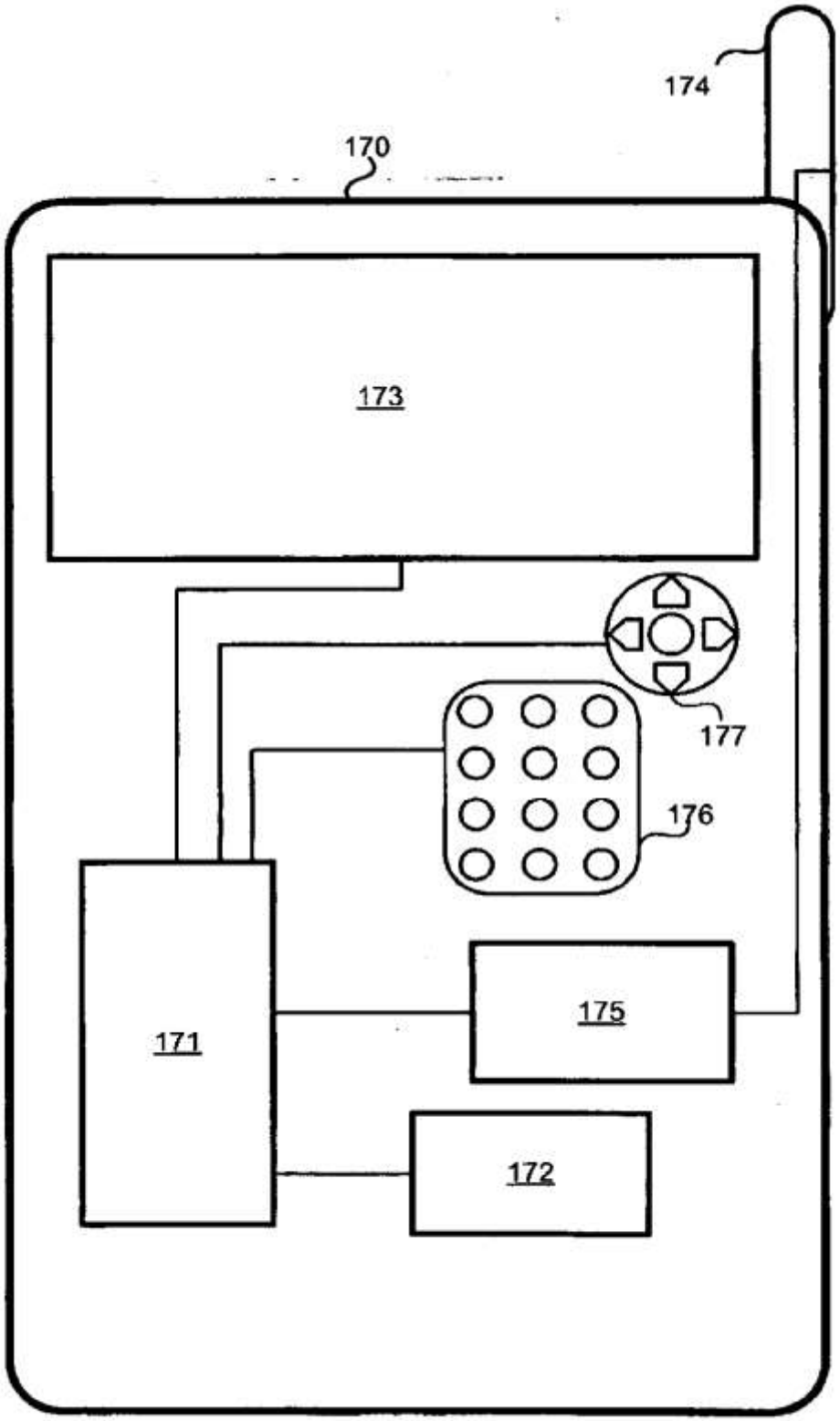

FIG. 7

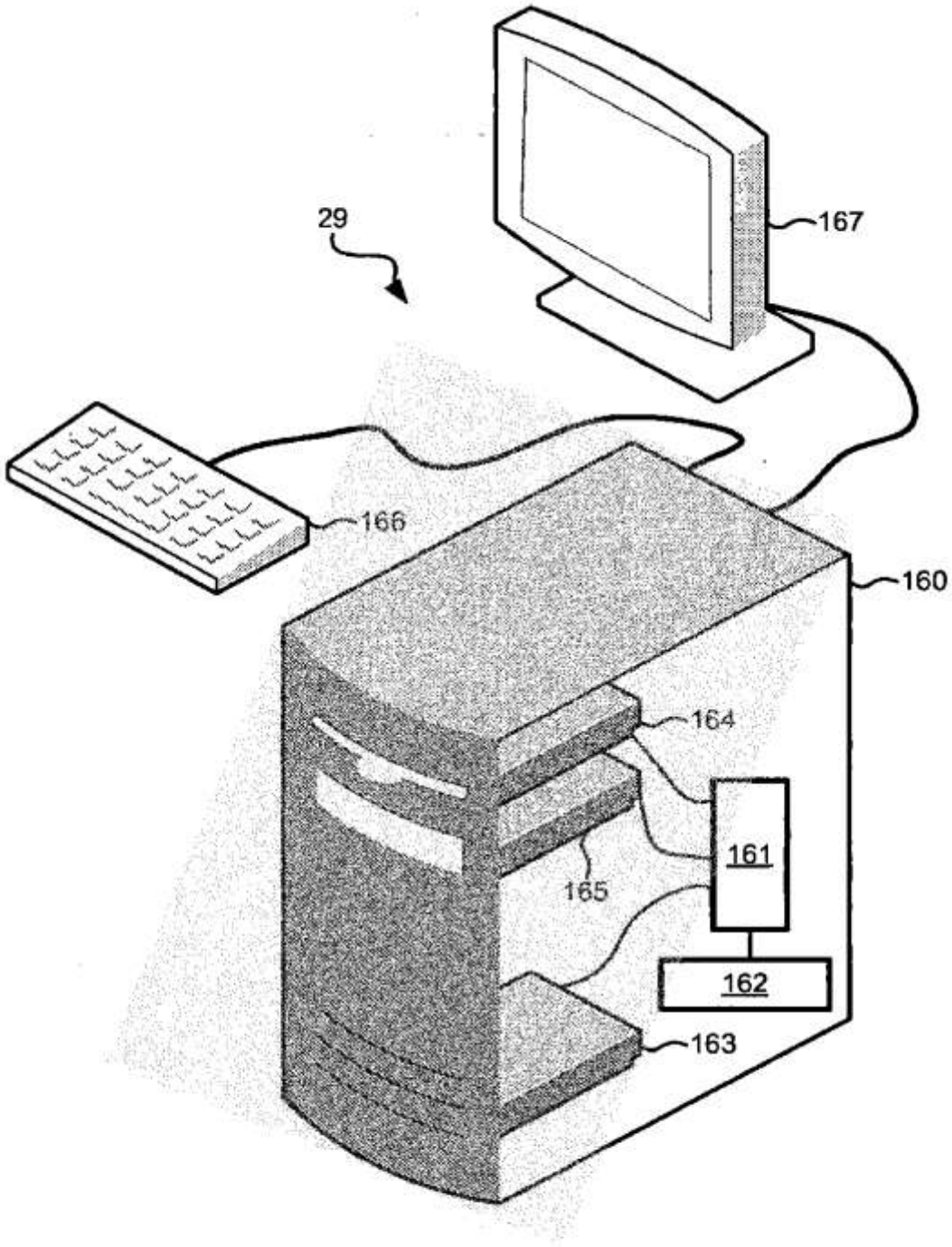

FIG. 8