(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 572 810**

(51) Int. CI.:

H04L 9/00 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.11.2004 E 04811786 (5)**

(97) Fecha y número de publicación de la concesión europea: **09.03.2016 EP 1692596**

(54) Título: **Descubrimiento y validación de rutas delegadas y distribuidas**

(30) Prioridad:

19.11.2003 US 523398 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.06.2016

(73) Titular/es:

ASSA ABLOY AB (100.0%)
Klarabergsviadukten 90
111 64 Stockholm, SE

(72) Inventor/es:

ENGBERG, DAVID

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Descubrimiento y validación de rutas delegadas y distribuidas.

Referencia cruzada a solicitudes relacionadas

La presente solicitud reivindica la prioridad con respecto a la solicitud provisional US 60/523.398 presentada el 19 de noviembre de 2003.

Antecedentes de la invención

1. Campo técnico

Esta solicitud se refiere al campo de la seguridad y la validación de datos, y más particularmente a un método para proporcionar información de validación de rutas para un sistema de acuerdo con el preámbulo de la reivindicación 1.

2. Descripción de las anterioridades

Resulta útil poder determinar el estado de un certificado digital, incluyendo la determinación de si el certificado se emitió de manera válida y/o si el certificado ha sido revocado antes de su expiración. Existen varias técnicas para determinar el estado de un certificado digital individual. Por ejemplo, las patentes US nº 5.666.416 y 5.717.758 describen técnicas para proporcionar el estado de un certificado individual. Se conocen también otras técnicas para diseminar y verificar el estado de un certificado, incluyendo Listas de Revocación de Certificados (CRL's), las cuales son listas firmadas digitalmente de certificados revocados.

En la verificación de un certificado digital puede que se requiera tener que confiar en el emisor del certificado digital y/o confiar en el firmante de la información de revocación, que puede ser o no la misma entidad. En el caso de un certificado digital, "confiar en" un emisor y/o un firmante de información de revocación puede referirse al hecho de que el emisor y/o el firmante sea una autoridad conocida que tenga una clave pública válida correspondiente a una clave secreta que fue utilizada para firmar el certificado y/o la información de revocación. Por ejemplo, un usuario puede recibir un certificado digital que esté firmado digitalmente por una autoridad, A, y puede recibir también una CRL actualizada (que no contiene el certificado digital) firmada por una autoridad diferente, A'. No obstante, el usuario desearía poder confiar tanto en A como en A' junto con sus claves públicas (correspondientes a las claves secretas utilizadas para firmar el certificado y la CRL) con el fin de poder respetar el certificado.

Existen mecanismos para facilitar la diseminación y la confianza de autoridades por otro lado desconocidas que emiten certificados e información de revocación. En algunas ocasiones, es posible hacer que una autoridad de confianza firme digitalmente información (o, de otra manera, que valide la información) para verificar una autoridad que de otro modo sería desconocida. Después de esto, la autoridad previamente desconocida puede presentar información firmada digitalmente (por ejemplo, un certificado digital y/o información de revocación) que se puede verificar utilizando la clave pública de la autoridad previamente desconocida. Por ejemplo, si un usuario no conoce o confía en la firma digital de las autoridades A1 y A2, pero el usuario sí conoce y confía en la autoridad A3, entonces el usuario puede obtener (o se le puede presentar) información firmada digitalmente por A3 (y por lo tanto avalada por A3) que indica que A1 y A2 son autoridades fiables. Así, si a dicho usuario se le presentasen un certificado digital firmado por A1 y una CRL (que no incluye el certificado digital) firmada por A2, el usuario utilizaría la información avalada por A3 para verificar la validez del certificado presentado.

Existen también mecanismos de anidamiento que se pueden utilizar en casos en los que autoridades avalan a otras autoridades. Por ejemplo, la patente US n. º 5.717.759 da a conocer una técnica en la que una primera autoridad, A1, avala una segunda autoridad, A2, la cual avala una tercera autoridad, A3, etcétera, hasta que el anidamiento llega a una autoridad en la que confía un hipotético usuario. En algunos casos, la acción de avalar puede incluir proporcionar una forma digital de la autoridad avaladora.

La patente US nº 6.134.550 da a conocer un método que construye una cadena de certificación preferida, tal como una lista de todas las autoridades de certificados en una ruta de confianza más corta, sobre la base de datos de cadenas de certificación generados, tales como una tabla de relaciones de confianza entre unidades emisoras de certificados en una comunidad de interés, con el fin de facilitar una rápida determinación de la validez del certificado por parte de una unidad solicitante. La unidad solicitante lleva a cabo una determinación de la validez sobre el certificado a validar, basándose en los datos de cadenas de certificados utilizando una o más bases de datos de directorios comunes o una versión de las mismas almacenada en memoria caché.

El documento "Delegated Path Validation and Delegated Path Discovery Protocol Requirements" de PINKAS, D. et al, ISSN: 0000-0003, especifica los requisitos para la Validación Delegada de Rutas (DPV) y el Descubrimiento Delegado de Rutas (DPD) para Certificados de Claves Públicas. Da a conocer la descarga de validación de rutas a un servidor y una validación de certificados en tiempo real.

La solicitud de patente US 2002/0046340 A1 da a conocer un centro de autenticación de validez de certificados VC que, de manera periódica, busca y verifica rutas que se extienden desde una autoridad de certificación puente a autoridades de certificación para admisión de terminales individuales, y que registra las rutas cuyas verificaciones siguen vigentes, en una base de datos de rutas en asociación con las respectivas autoridades de certificación para admisión de terminales.

Aunque el anidamiento y otros mecanismos son útiles, en algunos casos puede que a un usuario se le presenten un certificado digital y/o información de revocación y/o alguna otra información para los cuales no exista ningún mecanismo directo para determinar si se puede confiar en el firmante del certificado/información de revocación/otra información, y por lo tanto es posible que el usuario no pueda determinar si el certificado digital es válido en ese momento. Por consiguiente, resultaría útil afrontar esta cuestión.

Sumario de la invención

Dicho mecanismo directo para determinar si se puede confiar en el firmante del certificado/información de revocación/otra información se obtiene por el conjunto de las características de la reivindicación 1.

Según la presente invención, la provisión de información de validación de rutas para un sistema incluye determinar rutas entre un subconjunto de certificados del sistema y por lo menos un certificado raíz de confianza, almacenar cada una de las rutas en una tabla antes de una solicitud de información de validación de rutas, y extraer la información de validación almacenada en la tabla como respuesta a una solicitud de información de validación de rutas. La provisión de información de validación de rutas también puede incluir firmar digitalmente la información de validación. La provisión de información de validación de rutas también puede incluir aplicar restricciones a la información de validación y únicamente proporcionar información de validación que sea acorde con las restricciones. La determinación de rutas puede incluir construir un gráfico dirigido de raíces de confianza y del subconjunto de certificados, y llevar a cabo una búsqueda acíclica en profundidad del grafo. La tabla se puede indexar utilizando las raíces de confianza o utilizando los certificados. La provisión de información de validación de rutas también puede incluir recibir pruebas del estado de revocación para el subconjunto de certificados, almacenar las pruebas antes de una solicitud de información de validación de rutas, y extraer las pruebas junto con la información de validación como respuesta a una solicitud de información de validación de rutas. La provisión de información de validación de rutas también puede incluir firmar digitalmente la información de validación y las pruebas. La provisión de validación de rutas también puede incluir aplicar restricciones a la información de validación y únicamente proporcionar información de validación que esté acorde con las restricciones. La determinación de rutas puede incluir construir un grafo dirigido de raíces de confianza y del subconjunto de certificados, y llevar a cabo una búsqueda acíclica en profundidad del grafo. Las pruebas se pueden almacenar en la tabla que contiene la información de validación. La tabla se puede indexar utilizando las raíces de confianza. La tabla se puede indexar utilizando los certificados. Las pruebas se pueden almacenar en otra tabla que está separada de la tabla que contiene la información de validación. La otra tabla se puede indexar utilizando las raíces de confianza o utilizando los certificados. El subconjunto de certificados puede incluir raíces de confianza, autoridades que emiten certificados de usuario final, y autoridades que avalan otras autoridades. El subconjunto de certificados también puede incluir certificados de usuario final.

Todavía de acuerdo con la presente invención, un producto de programa de ordenador que proporcione información de validación de rutas para un sistema incluye un soporte de almacenamiento que contiene código ejecutable para el producto de programa de ordenador, código ejecutable que determina rutas entre un subconjunto de certificados del sistema y por lo menos un certificado raíz de confianza, código ejecutable que almacena cada una de las rutas en una tabla antes de una solicitud de información de validación de rutas, y código ejecutable que extrae la información de validación almacenada en la tabla como respuesta a una solicitud de información de validación de rutas. El producto de programa de ordenador también puede incluir código ejecutable que firma digitalmente la información de validación. El producto de programa de ordenador también puede incluir código ejecutable que aplica restricciones a la información de validación y que únicamente proporciona información de validación que es acorde con las restricciones. El código ejecutable que determina rutas puede construir un grafo dirigido de certificados raíz de confianza y del subconjunto de certificados, y puede llevar a cabo una búsqueda acíclica en profundidad del grafo. La tabla se puede indexar utilizando las raíces de confianza. La tabla se puede indexar utilizando los certificados. El producto de programa de ordenador también puede incluir código ejecutable que recibe pruebas del estado de revocación para el subconjunto de certificados, código ejecutable que almacena las pruebas antes de una solicitud de información de validación de rutas, y código ejecutable que extrae las pruebas junto con la información de validación como respuesta a una solicitud de información de validación de rutas. El producto de programa de ordenador también puede incluir código ejecutable que firma digitalmente la información de validación y las pruebas. El producto de programa de ordenador también puede incluir código ejecutable que aplica restricciones a la información de validación, y únicamente proporciona información de validación que es acorde con las restricciones. El código ejecutable que determina rutas puede construir un grafo dirigido de raíces de confianza y del subconjunto de certificados, y puede llevar a cabo una búsqueda acíclica en profundidad del grafo. Las pruebas se pueden almacenar en la tabla que contiene la información de validación. La tabla se puede indexar usando las raíces de confianza o utilizando los certificados. Las pruebas se pueden almacenar en otra tabla que está separada de la tabla que contiene la información de validación. La otra tabla se puede indexar utilizando las raíces de confianza o usando los certificados. El subconjunto de certificados puede incluir raíces de confianza, autoridades que emiten certificados

de usuario final, y autoridades que avalan a otras autoridades. El subconjunto de certificados también puede incluir certificados de usuario final.

Según todavía la presente invención, un servidor incluye un procesador, medios de almacenamiento internos acoplados al procesador, código ejecutable, proporcionado en los medios de almacenamiento internos, que determina rutas entre un subconjunto de certificados y por lo menos un certificado raíz de confianza, código ejecutable, proporcionado en los medios internos de almacenamiento, que almacena cada una de las rutas en una tabla antes de una solicitud de información de validación de rutas, y código ejecutable, proporcionado en los medios de almacenamiento internos, que extrae la información de validación almacenada en la tabla como respuesta a una solicitud de información de validación de rutas. El servidor puede incluir código ejecutable, proporcionado en los medios de almacenamiento internos, que firma digitalmente la información de validación. El servidor puede incluir código ejecutable, proporcionado en los medios de almacenamiento internos, que aplica restricciones a la información de validación, y que únicamente proporciona información de validación que es acorde con las restricciones. El código ejecutable que determina rutas puede construir un grafo dirigido de raíces de confianza y del subconjunto de certificados, y lleva a cabo una búsqueda acíclica en profundidad del grafo. La tabla se puede indexar utilizando las raíces de confianza o utilizando los certificados. El servidor puede incluir código ejecutable, proporcionado en los medios de almacenamiento internos, que recibe pruebas del estado de revocación para el subconjunto de certificados, código ejecutable, proporcionado en los medios internos de almacenamiento, que almacena las pruebas antes de una solicitud de información de validación de rutas, y código ejecutable, proporcionado en los medios de almacenamiento internos, que extrae las pruebas junto con la información de validación como respuesta a una solicitud de información de validación de rutas. El servidor puede incluir código ejecutable, proporcionado en los medios de almacenamiento internos, que firma digitalmente la información de validación y las pruebas. El servidor puede incluir código ejecutable, proporcionado en los medios de almacenamiento internos, que aplica restricciones a la información de validación y únicamente proporciona información de validación que es acorde a las restricciones. El código ejecutable que determina rutas puede construir un grafo dirigido de raíces de confianza y del subconjunto de certificados, y puede llevar a cabo una búsqueda acíclica en profundidad del grafo. Las pruebas se pueden almacenar en la tabla que contiene la información de validación. La tabla se puede indexar usando las raíces de confianza o utilizando los certificados. Las pruebas se pueden almacenar en otra tabla que esté separada de la tabla que contiene la información de validación. La otra tabla se puede indexar utilizando las raíces de confianza o usando los certificados. El subconjunto de certificados puede incluir raíces de confianza, autoridades que emiten certificados de usuario final, y autoridades que avalan a otras autoridades. El subconjunto de certificados también puede incluir certificados de usuario final.

Breve descripción de los dibujos

La Figura 1 ilustra un servidor no fiable de descubrimiento/validación delegados de rutas según una forma de realización del sistema que se describe en la presente.

La Figura 2 ilustra un servidor de confianza para descubrimiento/validación delegados de rutas según una forma de realización del sistema que se describe en la presente.

La Figura 3 ilustra dos áreas interconectadas, que contienen, cada una de ellas, información local de certificados según una forma de realización del sistema que se describe en la presente.

La Figura 4 ilustra el uso de una red para comunicar información de certificados a un usuario de acuerdo con una forma de realización del sistema que se describe en la presente.

La Figura 5 es un diagrama de flujo que ilustra el pre-cálculo de rutas de confianza según una forma de realización del sistema que se describe en la presente.

La Figura 6 es un diagrama de flujo que ilustra iteraciones a través de rutas de confianza en relación con el llenado de una tabla de certificados y rutas de confianza de acuerdo con el sistema que se describe en la presente.

Las Figuras 7A, 7B y 7C ilustran tablas que contienen rutas de confianza y/o pruebas de acuerdo con una forma de realización del sistema que se describe en la presente.

La Figura 8 es un diagrama de flujo que ilustra la devolución de rutas de confianza y/o pruebas pre-calculadas, según una forma de realización del sistema que se describe en la presente.

La Figura 9 es un diagrama de flujo que ilustra un procesado llevado a cabo por un servidor de confianza de descubrimiento/validación delegados de rutas según una forma de realización del sistema que se describe en la presente.

Descripción detallada de varias formas de realización

Se conocen técnicas para proporcionar información del estado de certificados individuales así como técnicas para verificar certificados y/o autoridades que firman digitalmente certificados. Véase, por ejemplo, la exposición que se proporciona en las patentes US nº 5.420.927; 5.604.804; 5.610.982; 6.097.811; 6.301.659; 5.793.868; 5.717.758; 5.717.575; 6.487.658; y 5.717.759. El sistema que se describe en la presente puede utilizar técnicas que se dan a conocer en una o más de estas patentes, posiblemente en combinación con otra u otras técnicas apropiadas. Las técnicas que se pueden utilizar incluyen, de manera individual o en cualquier combinación, CRL's completas, CRL's con particiones, CRL's delta, respuestas de OCSP (individualmente y por grupos), mini CRL's (CRL's comprimidas a nivel de bits), VTokens (cadena *hash* unidireccional), y diversas versiones de árboles de Merkle o de otros árboles.

Descubrimiento de rutas se refiere al proceso de encontrar una ruta de confianza (relación de confianza) entre un certificado arbitrario y una de entre las raíces de confianza de un usuario, los cuales son certificados digitales que se corresponden con autoridades en las que confía un usuario. Una ruta de confianza es una cadena de autorizaciones desde un certificado a otro con un certificado de destino en un extremo y un certificado raíz de confianza en el otro. Por ejemplo, si el certificado C1 se corresponde con una autoridad de confianza A1, y A1 firma C2 para la autoridad desconocida A2 y la autoridad A2 firma el certificado C3 para la autoridad desconocida A3 que firmó el certificado de destino, entonces una ruta de confianza desde C1 (el certificado raíz de confianza) al certificado de destino es C1 a C2, C2 a C3, y C3 al certificado de destino.

En algunos casos, el descubrimiento de rutas se puede llevar a cabo localmente de una manera bastante directa por parte del usuario siempre que todos los certificados de una ruta de confianza estén disponibles localmente. No obstante, en algunos casos, incluyendo aquellos con un modelo de confianza federado que se basa en la certificación cruzada, puede que los usuarios no dispongan de toda la información necesaria para llevar a cabo un descubrimiento de rutas local.

Obsérvese también que, incluso cuando se ha encontrado una ruta de confianza completa entre un certificado raíz de confianza y un certificado de destino, puede seguir existiendo la inquietud de que se puedan haber revocado uno o más de los certificados sobre la ruta de confianza desde la emisión de los mismos. Validación de rutas se refiere a la confirmación del estado actual de todos los certificados en una ruta de confianza, incluyendo su validez (estado de revocación) de los certificados y teniendo en cuenta cada una de las reglas y/o restricciones correspondientes al uso de los certificados (por ejemplo, comprobación de políticas de seguridad). El ensamblaje de la información de estados de revocación para cada certificado en la ruta de confianza puede resultar relativamente difícil para algunos usuarios en algunas situaciones (por ejemplo, aquellas correspondientes a valores de configuración de cortafuegos especiales que eviten el acceso a redes públicas). Por consiguiente, es útil poder proporcionar un servicio que pueda verificar un certificado en una única transacción. Esto se puede realizar en primer lugar determinando la ruta de confianza, recibiendo información de revocación (y/o información de restricciones) sobre los certificados en la ruta de confianza, y procesando la información recibida para verificar el certificado de destino.

En referencia a la Figura 1, un servidor no fiable de descubrimiento/validación delegados de rutas (UDPDV) 30 recibe, como entrada, información que identifica uno o más raíces de confianza (certificados correspondientes a autoridades de confianza) y un identificador correspondiente a un certificado de destino (o quizás alguna otra información/datos) que desea validar un usuario. Opcionalmente, el servidor de UDPDV 30 se puede preconfigurar con raíces de confianza además de recibir como entrada raíces de confianza, o de manera alternativa a esto último.

Evidentemente, si el usuario ya confía en una autoridad que emitió el certificado de destino y el usuario tiene acceso a información de revocación fiable para el certificado de destino (y posiblemente el certificado de la autoridad de confianza), entonces el usuario puede verificar el certificado de destino con esa información, y puede que no sea necesario utilizar el servidor de UDPDV 30. Por consiguiente, el servidor de UDPDV 30 es útil en casos en los que un usuario desea verificar el estado de un certificado de destino para el cual el usuario no confía en (no conoce) la autoridad que emitió el certificado de destino y/o para el cual el usuario no posee información de revocación fiable sobre el certificado de destino (y posiblemente el certificado de la autoridad que emitió el certificado de destino).

El servidor de UDPDV 30 procesa las entradas que van hacia el mismo, para determinar una o más rutas de confianza entre el certificado de destino y un certificado raíz de confianza (o bien introducido o bien preconfigurado en el servidor de UDPDV 30, según se ha descrito anteriormente). Obsérvese que, en muchos casos, también puede resultar útil confirmar que no se ha revocado ninguno de los certificados en una ruta de confianza (lo cual indica, por ejemplo, compromiso de la clave secreta de una autoridad). En tal caso, puede resultar útil hacer que el servidor de UDPDV 30 también proporcione pruebas en forma de información de revocación autenticada (por ejemplo, CRL's o respuestas de OCSP). Por consiguiente, en algunas formas de realización, el servidor de UDPDV 30 también puede proporcionar pruebas para certificados en una ruta de confianza.

Así, en la forma de realización que se da a conocer en la Figura 1, el servidor de UDPDV 30 ensambla la información de rutas de confianza para el certificado de destino y, opcionalmente, también ensambla información de revocación para elementos de la ruta. La salida del servidor de UDPDV 30 hacia el usuario no se puede autenticar (por ejemplo, firmar) independientemente. Por el contrario, el servidor de UDPDV 30 devuelve todos los elementos

individuales de la ruta de confianza (y, opcionalmente, pruebas) al usuario, el cual a continuación puede verificar independientemente la corrección de la ruta de confianza y la validez de sus elementos (certificados). El funcionamiento del servidor de UDPDV 30 se describe de forma más detallada en otras secciones del presente documento.

En referencia a la Figura 2, un servidor de confianza para descubrimiento/validación delegados de rutas 40 recibe, como entrada, raíces de confianza de un usuario y un identificador correspondiente a un certificado de destino (o quizás alguna otra información/datos) que desea verificar un usuario. Opcionalmente, el servidor de confianza para descubrimiento/validación delegados de rutas 40 se puede pre-configurar con raíces de confianza además de recibir las raíces de confianza como entrada, o de manera alternativa a esto último.

El servidor de confianza para descubrimiento/validación delegados de rutas 40 da salida a un resultado que indica si el certificado de destino (u otra información/datos) es o no válido. En una forma de realización que se describe en la presente, el servidor 40 lleva a cabo su propia autenticación criptográfica de la información que se proporciona al usuario. En esta forma de realización, el servidor 40 puede firmar respuestas proporcionadas de este modo, lo cual permitiría que el servidor 40 proporcionase un pequeño volumen de datos al usuario (por ejemplo, “Sí, puede confiar en el certificado X”). No obstante, una implementación de este tipo prevé que el usuario confíe explícitamente en la integridad y la corrección de las operaciones internas del servidor de confianza para descubrimiento/validación delegados de rutas 40. Si el servidor 40 se ve comprometido, el servidor 40 se podría utilizar de manera inadecuada para autenticar respuestas que validan cualquier certificado, con independencia del origen o el estado actual.

Los servidores 30, 40 se pueden proporcionar mediante estaciones de trabajo informáticas que tengan procesadores y medios internos de almacenamiento para almacenar código ejecutable y datos, uno o más módulos de software proporcionados en un ordenador de propósito general, hardware dedicado, o cualquier combinación de hardware y software con capacidad de proporcionar la funcionalidad que se describe en la presente. Para el sistema descrito en este documento, el servidor de UDPDV 30 se puede proporcionar por medio de uno o más servidores ligeros que no necesitan tener capacidades de autenticación (por ejemplo, claves privadas para firmas digitales).

El servidor de UDPDV 30 se puede configurar periódicamente con listas de información de dos tipos. El primer tipo de lista contiene un conjunto de certificados que se pueden usar en la validación de rutas y, en una forma de realización de la presente, representa todos o prácticamente todos los certificados accesibles (por ejemplo, por medio de una red) para el servidor de UDPDV 30. En otra forma de realización, el primer tipo de lista contiene certificados únicamente para autoridades que emiten certificados e información de revocación, y para autoridades que abalan a dichas autoridades, sin contener necesariamente la totalidad o ni siquiera ninguno de los certificados de usuario final. El primer tipo de listas puede contener certificados raíz autofirmados (certificados raíz de confianza) que actúan como anclas de confianza. Los certificados raíz de confianza pueden ser firmados por autoridades en las que confía(n) el(los) usuario(s) del sistema. El primer tipo de listas también puede contener certificados del emisor (también conocido como “autoridad de certificación”) para autoridades que emiten certificados, autoridades que emiten información de revocación, y/o autoridades que avalan a otras autoridades. En una forma de realización, el primer tipo de listas también puede contener certificados de usuario final mientras que en otra forma de realización, el primer tipo de listas no contiene certificados de usuario final. El primer tipo de listas de certificados se puede usar para proporcionar servicios de descubrimiento de rutas, según se describe en la presente.

El segundo tipo de lista proporcionado en el servidor de UDPDV 30 puede incluir pruebas pregeneradas del estado del certificado. Cada prueba puede contener el estado de uno o más certificados (de la primera lista) para un intervalo de tiempo fijado, y la prueba se puede autenticar de manera segura, por ejemplo utilizando una firma digital. Las pruebas se pueden usar para proporcionar servicios de validación de rutas, según se describen en alguna otra sección en el presente documento. Las pruebas pueden ser proporcionadas por cualesquiera medios apropiados, incluyendo CRL’s, respuestas de OCSP, VTokens, etcétera.

La comprobación de una ruta entre un certificado raíz de confianza y un certificado de destino es conocida en la técnica y está bien documentada en las normativas sobre certificados (por ejemplo, RFC 3280). No obstante, el tiempo que se tarda en encontrar una ruta de confianza sobre un número elevado de certificados puede aumentar de manera exponencial según el número de certificados del grupo. Esto puede resultar aceptable en algunas situaciones y/o para pequeñas colecciones de certificados, aunque puede ser inaceptable en otras situaciones, tales como una gran comunidad de autoridades federadas.

El sistema descrito en la presente está diseñado para llevar a cabo el descubrimiento de rutas en tiempo logarítmico o constante en el momento de una solicitud de descubrimiento, en primer lugar pre-calculando rutas de confianza entre cada certificado raíz de confianza y la totalidad del resto de certificados accesibles, para autoridades que emiten certificados y/o avalan a otras autoridades. Cuando el servidor de UDPDV 30 recibe una lista nueva de certificados (o se acopla a una fuente de certificados nuevos), el servidor puede pre-calcular una matriz de M por N donde M es el número de raíces de confianza y N es el número total de certificados. Cada celda de la matriz (por ejemplo, en la fila r1 y columna c1) puede contener una o más rutas legítimas desde el certificado raíz de confianza específico indicado por la fila r1 al certificado específico indicado por la columna c1, o si no, puede contener un

conjunto vacío para indicar que no es posible ninguna ruta. Opcionalmente, cada celda (o cada celda de una tabla análoga) también puede contener pruebas apropiadas para proporcionar la validación.

Cuando llega una solicitud de usuario para verificar un certificado de destino, el servidor de UDPDV 30 utiliza la matriz pre-calculada para buscar el(los) certificado(s) de confianza para el usuario y para buscar la autoridad que emitió el certificado de destino y, opcionalmente, una autoridad que emitió información de revocación para el certificado de destino (en caso de que sea diferente de la autoridad emisora) para hallar una o más rutas válidas entre ellas. Esto se puede llevar a cabo en una búsqueda en tiempo constante puesto que las rutas se han pre-calculado y almacenado en el servidor de UDPDV 30. Obsérvese que si hay más de una ruta de confianza posible o si hay restricciones asociadas a una ruta de confianza (por ejemplo, restricciones de nombres o políticas) que limitan en cualquier modo el uso de cualquiera de los certificados en la ruta de confianza, entonces es necesario aplicar las políticas de rutas con respecto a cualquier(cualesquiera) ruta(s) de confianza encontrada(s). Al pre-calcular todas las rutas posibles, el servidor de UDPDV 30 puede ofrecer descubrimiento de rutas para grandes comunidades con un rendimiento y una escalabilidad relativamente altos.

Además del descubrimiento de rutas, el servidor de UDPDV 30 también puede proporcionar información de validación (pruebas) para elementos (certificados) de una ruta de confianza. En una forma de realización, el servidor de UDPDV 30 obtiene las pruebas (por ejemplo, en forma de una CRL o una respuesta de OCSP) en tiempo real para cada elemento (certificado) de una ruta de confianza que a continuación se proporciona al usuario. Aunque puede resultar posible mejorar el rendimiento almacenando pruebas en memoria caché, puede seguir habiendo potencial para un rendimiento no óptimo en el momento de una solicitud cuando se obtienen pruebas en tiempo real. En otra forma de realización, puede haber un mecanismo de validación de rutas en el servidor de UDPDV 30 que reciba a intervalos regulares, pruebas de estado detalladas, pregeneradas, para cada certificado utilizado por el servidor de UDPDV 30 en relación con la generación de rutas de confianza. Para esta forma de realización, el servidor de UDPDV 30 puede tener la capacidad de acceder rápidamente a toda la información de validación necesaria que se puede proporcionar a partes que confían sin requerir ningún tiempo de procesado adicional para recuperar la información del estado del certificado para su validación en tiempo real.

Obsérvese también que, si las pruebas se envían sin solicitud previa (*pushed*) al servidor de UDPDV 30 (por ejemplo, en forma de respuestas de OCSP pre-firmadas), el servidor de UDPDV 30 puede tener acceso local instantáneo al estado de cada certificado en una ruta de confianza. Para algunas formas de realización, el servidor de UDPDV 30 confirma el estado de la ruta de confianza antes de devolver la ruta de confianza para la delegación de rutas. El servidor de UDPDV 30 opcionalmente también puede devolver las pruebas de estado al usuario para permitir una validación completa local de la ruta de confianza por parte del usuario. La naturaleza individualizada, pregenerada, de las pruebas (por ejemplo, respuestas de OCSP pregeneradas) puede permitir un uso eficiente de recursos de red, al mismo tiempo que evita cualesquiera riesgos de seguridad que se puedan asociar a servidores en línea, de confianza.

En referencia a la Figura 3, un diagrama 50 muestra una primera área 52 y una segunda área independiente 54. Las áreas 52, 54 se pueden interconectar por cualesquiera medios apropiados (por ejemplo, una red o conexión directa) para permitir un intercambio de señales entre ellas. La primera área 52 incluye una pluralidad de certificados 62 a 64. La segunda área 54 incluye una pluralidad de certificados diferentes 66 a 68. La primera área 52 representa una localidad que puede ser gestionada y a la que puede acceder localmente un usuario de ella. De manera similar, la segunda área 54 representa una localidad separada que puede ser gestionada y a la que puede acceder localmente un usuario diferente en ella. Así, por ejemplo, un usuario del área 52 puede acceder localmente a cualquiera o a la totalidad de los certificados 62 a 64.

En el área 52, el certificado 62 es un certificado raíz (certificado raíz de confianza) auto-certificatorio para una autoridad A1. El certificado 62 también certifica el certificado 63 para una autoridad A2, por ejemplo, haciendo que A1 firme el certificado 63. El certificado 63 certifica el certificado 64 para una autoridad A3. Obsérvese que, en este ejemplo, si un usuario confía en A1, entonces el usuario también debería confiar en A2 (avalada por A1) y también debería confiar en A3 (avalada por A2). En el área 54, el certificado 66 es un certificado raíz auto-certificatorio (certificado raíz de confianza) para una autoridad A1'. El certificado 66 también certifica al certificado 67 para una autoridad A2', y el certificado 67 certifica al certificado 68 para una autoridad A3'. El certificado 62 se certifica de manera cruzada con el certificado 66, de manera que cada uno de los certificados 62, 66 certifica el otro de los certificados 62, 66.

Si a un usuario en el área 52 se le presenta un certificado de destino firmado por A3', es posible que el usuario no pueda verificar inmediatamente que el certificado de destino es válido en caso de que el usuario del área 52 inicialmente solo tenga conocimiento sobre (y confíe en) A1, A2 y A3. No obstante, obsérvese que la autoridad A2' avala a la autoridad A3', y que la autoridad A1' avala a la autoridad A2'. Obsérvese también que la autoridad A1 avala a la autoridad A1'. Así, suponiendo que un usuario local en el área 52 confía en A1, entonces existe una ruta de confianza para el usuario desde el certificado 62 al certificado 66 al certificado 67 hacia el certificado 68 hasta el certificado de destino que ha sido firmado por A3'. De este modo, el usuario puede aceptar el certificado de destino firmado por la autoridad A3' gracias a la ruta de confianza desde el certificado de destino al certificado 62 que ha sido firmado por la autoridad de confianza A1. Así mismo, tal como se describe en alguna otra sección en la

presente, es posible proporcionar información de validación (prueba de validez) para cada uno de los certificados a lo largo de la ruta de confianza, así como para cualquier autoridad que emitiese información de revocación (en caso de que fuese diferente de la autoridad emisora) de manera que, en el ejemplo el usuario que recibe la ruta de confianza también puede recibir información de revocación actualizada para los certificados 62, 66 a 68.

En referencia a la Figura 4, un diagrama 80 ilustra un usuario 82 que recibe información de certificación (e incluye información de rutas de confianza y posiblemente información de validación) desde uno o más de una pluralidad de dispositivos de almacenamiento de datos 84-86 acoplados al usuario 82 por medio de una red 88. En una forma de realización de la presente, la red 88 puede ser Internet, aunque pueden utilizarse otras redes adecuadas, incluyendo redes que proporcionan conexiones directas entre el usuario y uno o más de los dispositivos de almacenamiento de datos 84-86. Obsérvese también que el usuario 82 puede almacenar localmente alguna información de certificación. En una forma de realización de la presente, al usuario 82 se le pueden presentar uno o más certificados cuya validez desea determinar el usuario. En algunos casos, el usuario 82 puede determinar la validez de los certificados utilizando datos locales. No obstante, tal como se describe en alguna otra sección en la presente, puede que sea necesario en otros casos, que el usuario 82 obtenga información de certificación de otras fuentes como los dispositivos de almacenamiento de datos 84-86. En tales casos, entre el usuario y los dispositivos de almacenamiento 84-86, a través de la red 88 y de una manera directa, se pueden comunicar información de certificación y solicitudes de la misma. Evidentemente, para proporcionar la funcionalidad que se describe en la presente pueden utilizarse cualesquiera técnicas apropiadas de transmisión/solicitud de información y de conectividad.

En referencia a la Figura 5, un diagrama de flujo 100 ilustra la inicialización del servidor de UDPDV 30 para que contenga todas las rutas entre las raíces de confianza (certificados raíz de autoridades de confianza) y otro u otros certificados que emiten certificados y/o avalan otras autoridades. Tal como se describe en alguna otra sección en la presente, cada una de las rutas de confianza se puede pre-calcular de manera que cuando un usuario presenta un certificado de destino, el servidor de UDPDV puede consultar una tabla, buscar la autoridad que emitió el certificado de destino (o buscar el propio certificado de destino), y proporcionar una ruta de confianza pre-calculada desde el certificado de destino a un certificado raíz de confianza. Tal como también se describe en la presente, el servidor de UDPDV 30 puede proporcionar opcionalmente, para los certificados en la ruta de confianza, pruebas que indican que los certificados no han sido revocados.

El procesado para el diagrama de flujo 100 comienza en una primera etapa 102 en la que se construye un grado dirigido para todos los certificados para los cuales se va a almacenar información. Un grafo dirigido es un constructo matemático que es bien conocido en la técnica. Para una forma de realización de la presente, se usan todos los certificados de un sistema, incluyendo certificados de usuario final. Para otra forma de realización, no se incluyen certificados de usuario final o, alternativamente, se incluyen únicamente algunos certificados de usuario final. En la etapa 102, el grafo dirigido que se construye representa una relación de confianza entre certificados donde una arista (línea de conexión) de grafo indica que una primera autoridad (correspondiente a un certificado conectado por un extremo de la arista) ha avalado a una segunda autoridad (correspondiente a un certificado conectado por el otro extremo de la arista).

Después de la etapa 102, se encuentra una etapa 104 en la que una variable a modo de índice, I, se fija igual a uno. La variable a modo de índice, I, se utiliza para realizar iteraciones a través de cada uno de los certificados raíz de confianza para el servidor de UDPDV 30. Tal como se describe en alguna otra sección de la presente, los certificados raíz de confianza se proporcionan como entrada al servidor de UDPDV 30 o están pre-configurados en este último.

Después de la etapa 104 se encuentra una etapa de prueba 106 en la que se determinan si la variable a modo de índice, I, es mayor que el número de certificados raíz de confianza. En caso afirmativo, entonces se ha completado el procesado. En caso contrario, el control se transfiere desde la etapa de prueba 106 a una etapa 108 para determinar todas las rutas desde el certificado raíz de confianza (correspondiente a la variable a modo de índice I) a la totalidad del resto de certificados en el grafo dirigido. La etapa 108 se describe de forma más detallada en algún otro lugar de la presente. Después de la etapa 108 se encuentra una etapa 112 en la que se incrementa la variable a modo de índice, I. Después de la etapa 112, el control se transfiere de vuelta a la etapa de prueba 106, descrita anteriormente.

En referencia a la Figura 6, un diagrama de flujo 120 ilustra más detalladamente el procesado que se lleva a cabo en relación con la etapa 108 del diagrama de flujo 100 de la Figura 5. Para cada una de las raíces de confianza, se lleva a cabo una búsqueda acíclica en profundidad del grafo dirigido para encontrar todas las rutas de confianza. Para cada certificado que se encuentra en cada ruta, se materializa una entrada en una tabla que indica la ruta de confianza desde el certificado al certificado raíz de confianza.

El procesado comienza en una primera etapa 122, en la que se determina si hay más rutas a examinar. Obsérvese que, en algunas ocasiones, puede ser posible que exista un certificado raíz de confianza sin ninguna ruta hacia el mismo. No obstante, en la mayoría de los casos, se espera que cada una de las raíces de confianza tenga por lo menos una ruta hacia la misma. Si en la etapa de prueba 122 se determina que no hay más rutas a examinar

(procesar), entonces el procesado se ha completado. En caso contrario, el control se transfiere desde la etapa de prueba 122 a una etapa 124 en la que se determina la siguiente ruta utilizando la búsqueda acíclica en profundidad del grafo dirigido. Después de la etapa 124 se encuentra una etapa 126 en la que un puntero de certificados, CP, se fija de manera que apunte al extremo de la ruta que se está examinando (procesando).

Después de la etapa 126 se encuentra una etapa de prueba 128 que determina si el CP apunta al certificado raíz de confianza, indicando así que se ha recorrido la ruta completa. En caso afirmativo, entonces el control se transfiere desde la etapa de prueba 128 de vuelta a la etapa 122, descrita anteriormente, para dar inicio a la siguiente iteración. Si no, el control se transfiere desde la etapa de prueba 128 a una etapa 132 en la que la ruta desde CP al certificado raíz de confianza se registra en la tabla (descrita en alguna otra sección en la presente) que almacena certificados y rutas de confianza hacia los mismos. En una forma de realización, en una parte de la tabla indexada por el certificado al que apunta CP, se registra en la etapa 132 la ruta desde CP al certificado raíz de confianza. Después de la etapa 132 se encuentra una etapa 134 en la que CP se fija de manera que apunte al certificado previo en la ruta. Así, CP inicialmente apunta al extremo de la ruta y a continuación apunta posteriormente a certificados previos de la ruta yendo hacia atrás en dirección al certificado raíz de confianza. Después de la etapa 134, el control se transfiere de nuevo a la etapa de prueba 128, descrita anteriormente.

En referencia a la Figura 7A, una tabla 140 incluye una primera parte 142 indexada por certificados del sistema y que tiene, como elementos, rutas de confianza a cada uno de los certificados. La tabla 140 también puede incluir una segunda parte 144 que también está indexada por certificados del sistema. La segunda parte tiene elementos que describen pruebas (por ejemplo, respuestas de OCSP, CRL's, etcétera) que indican el estado de revocación para cada uno de los certificados correspondientes. En una forma de realización que se describe en la presente, las pruebas proporcionadas en la segunda parte 144 se corresponden con el certificado del índice de manera que, por ejemplo, la entrada de la tabla indexada por C2 se corresponde con una prueba para C2. En otra forma de realización, las pruebas proporcionadas en la segunda parte 144 se corresponden con todos los certificados de todas las rutas para una entrada particular de la primera parte 142. Así, por ejemplo, las pruebas proporcionadas en la segunda parte 144 en relación con el certificado C2 se corresponden con todos los certificados de las rutas de confianza proporcionadas en la entrada para C2 en la primera parte 142.

En algunas formas de realización, puede que resulte posible eliminar una de las partes 142, 144. Así, por ejemplo, en formas de realización con solamente la parte 142, el servidor de UDPDV 30 proporciona rutas de confianza pre-calculadas, aunque no pruebas. Para dichas formas de realización, los usuarios o bien pueden renunciar a las pruebas en su totalidad, o bien obtener pruebas en tiempo real, o alguna combinación de estas opciones (es decir, obtener pruebas para algunos certificados de las rutas pero no para otros). Para formas de realización con solamente la parte 144, se pueden determinar rutas de confianza en tiempo real y las pruebas pre-calculadas de la parte 144 pueden ser proporcionadas por el servidor de UDPDV 30.

En referencia a la Figura 7B, otra forma de realización utiliza una única tabla 140' indexada de acuerdo con certificados, en donde tanto las rutas de confianza como las pruebas se proporcionan como elementos de la tabla 140'.

En referencia a la Figura 7C, todavía otra forma de realización ilustra otra configuración para la tabla 140''. La tabla 140'' se puede indexar de acuerdo con un certificado raíz de confianza particular TR1, TR2... TRN y otros certificados C1, C2,... CN. Los elementos de una entrada de la tabla 140'' contienen rutas de confianza y (opcionalmente) pruebas "P/P" de manera que, por ejemplo, una entrada correspondiente al certificado raíz de confianza TRx y el certificado Cy contiene una o más rutas de confianza (si es que existe alguna) desde Cy a TRx y, opcionalmente, una o más pruebas para solamente Cy (en una forma de realización) o para todos los certificados de la(s) ruta(s) de confianza (en otra forma de realización).

En referencia a la Figura 8, un diagrama de flujo 150 ilustra etapas para el procesado en relación con el servidor de UDPDV 30 que presta servicio a una solicitud proveniente de un usuario en relación con una ruta de confianza y, opcionalmente, pruebas para sus certificados. Tal como se describe en algún otro lugar de la presente, al servidor de UDPDV 30 se le puede presentar un certificado de destino particular para el cual el servidor de UDPDV 30 proporciona una ruta de confianza y opcionalmente pruebas que indican el estado de cada certificado en la ruta de confianza. En una forma de realización, la ruta de confianza se proporciona a un certificado para una autoridad que emitió el certificado de destino y, opcionalmente, a un certificado para una autoridad que emitió información de revocación para el certificado de destino (en caso de que sea diferente de la autoridad emisora). En otra forma de realización, el servidor de UDPDV 30 proporciona una ruta de confianza e información de revocación opcional para el propio certificado de destino.

El procesado comienza en una primera etapa 152 en la que se determina si hay alguna ruta de confianza disponible para el certificado de destino o su emisor. En caso negativo, entonces el control se transfiere desde la etapa 152 a una etapa 154 en la que se lleva a cabo un procesado especial. El procesado especial que se lleva a cabo en la etapa 154 puede incluir publicar un mensaje de error y/o indicar a un usuario de alguna otra manera, que no se ha encontrado ninguna ruta de confianza para el certificado de destino. Después de la etapa 154 se ha completado el procesado.

Si en la etapa de prueba 152 se determina que hay rutas de confianza disponibles, entonces el control se transfiere desde la etapa de prueba 152 a una etapa 156 en la que se selecciona la siguiente ruta de confianza para el procesado. En una forma de realización de la presente, el sistema puede realizar iteraciones a través de cada una de las rutas de confianza (proporcionadas por la tabla 140, la tabla 140', o la etapa 140'') para encontrar una ruta de confianza apropiada entre el certificado de destino (o su emisor) y uno o más de los certificados raíz de confianza. La siguiente ruta de confianza escogida en la etapa 156 se puede seleccionar utilizando cualquiera de entre varios criterios posibles, tales como la ruta más corta, una ruta que contiene certificados particulares, etcétera.

Después de la etapa 156 se encuentra una etapa de prueba 158 que determina si existen restricciones sobre la ruta de confianza particular (certificados de la ruta de confianza) seleccionada en la etapa 156. Tal como se describe en alguna otra sección de la presente, puede haber una o más restricciones que eviten el uso de una ruta de confianza particular, tales como, por ejemplo, que uno o más certificados no sean aceptables para ciertas finalidades. Si en la etapa de prueba 158 se determina que existen restricciones que hacen que la ruta de confianza que se está examinando sea inaceptable, entonces el control se transfiere desde la etapa de prueba 158 de vuelta a la etapa 152, descrita anteriormente. En caso contrario, el control se transfiere desde la etapa de prueba 158 a una etapa 162 en la que se determina si se han solicitado pruebas para los certificados en la ruta de confianza. En caso negativo, entonces el control se transfiere desde la etapa 162 a una etapa 164 en la que la ruta de confianza entre el certificado de destino (o su emisor) y el certificado raíz de confianza se devuelve al usuario. Después de la etapa 164 se ha completado el procesado.

Si en la etapa de prueba 162 se determina que se han solicitado pruebas, entonces el control se transfiere desde la etapa de prueba 162 a una etapa 166 en la que se obtienen las pruebas (a partir de la tabla 140, la tabla 140', o la tabla 140''). En otras formas de realización, las pruebas se pueden obtener en tiempo real. Después de la etapa 166 se encuentra una etapa 168 en la que se devuelven la ruta de confianza y las pruebas. Después de la etapa 168 se ha completado el procesado.

Tal como se describe en alguna otra sección de la presente, en algunos casos, puede que un usuario desee utilizar el servidor 40 de confianza para descubrimiento y validación delegados y distribuidos de rutas, que devuelve un mensaje firmado (o autenticado de alguna otra manera) que indica si un certificado particular es o no válido. El servidor 40 puede firmar un mensaje que indica que un certificado particular es aceptable o no. El usuario puede basarse en la respuesta firmada de servidor 40 sin conocer o examinar necesariamente la ruta y/o la información de validación de primera mano.

En referencia a la Figura 9, un diagrama de flujo 180 ilustra etapas llevadas a cabo por el servidor 40 en relación con la construcción y la devolución de un mensaje firmado que indica que un certificado de destino particular es o no válido. El procesado comienza en una primera etapa 182 en la que la ruta de confianza y las pruebas se obtienen de acuerdo con la descripción ofrecida en alguna otra sección de la presente. Después de la etapa 182 se encuentra una etapa de prueba 184 en la que se examinan la ruta de confianza y las pruebas para determinar si el certificado de destino es válido. La determinación de la etapa 184 se puede efectuar utilizando la ruta de confianza y pruebas obtenidas en la etapa 182. Si en la etapa de prueba 184 se determina que el certificado de destino es válido, entonces el control se transfiere desde la etapa de prueba 184 a una etapa 186 en la que se crea un mensaje positivo, que indica que el certificado de destino es válido. En caso contrario, si en la etapa de prueba 184 se determina que el certificado de destino no es válido, entonces el control se transfiere desde la etapa de prueba 184 a una etapa 188 en la que se crea un mensaje negativo.

Después o bien de la etapa 186 ó bien de la etapa 188 se encuentra una etapa 192 en la que el mensaje es firmado digitalmente por el servidor 40. Tras la etapa 192 se encuentra una etapa 184 en la que el resultado firmado se devuelve al usuario. Después de la etapa 194 el procesado se ha completado.

El sistema descrito en la presente se puede implementar utilizando cualquier combinación apropiada de hardware y/o software, incluyendo software proporcionado en un soporte de almacenamiento (por ejemplo, un disco, una cinta, un CD ROM, una memoria extraíble, etcétera). El software se puede ejecutar sobre hardware especializado, en un ordenador de propósito general, o una combinación apropiada de los mismos.

Aunque la invención se ha dado a conocer en relación con diversas formas de realización, se pondrán de manifiesto fácilmente modificaciones de las mismas para aquellos versados en la materia. Por consiguiente, el alcance de la invención se expone en las siguientes reivindicaciones.

REIVINDICACIONES

1. Método para proporcionar información de validación de rutas para un sistema, que comprende:

determinar (108, 124) unas rutas de confianza entre un subconjunto de certificados del sistema y por lo menos una raíz de confianza, incluyendo dichas rutas de confianza una cadena de autorizaciones desde un certificado de destino a dicho por lo menos un certificado raíz de confianza;

almacenar (132) cada una de las rutas de confianza en una tabla antes de una solicitud de información de validación de rutas;

recibir (182) unas pruebas del estado de revocación para dicho subconjunto de certificados;

caracterizado por que comprende las etapas siguientes:

pregenerar dichas pruebas;

firmar digitalmente dichas pruebas;

almacenar dichas pruebas antes de una solicitud de información de validación de rutas, siendo las pruebas apropiadas para proporcionar validación; y

extraer las rutas de confianza almacenadas en la tabla y las pruebas pregeneradas almacenadas como respuesta a una solicitud de información de validación de rutas sin recuperar la información de estado de revocación en tiempo real.

2. Método según la reivindicación 1, que además comprende:

aplicar restricciones a la información de validación y proporcionar únicamente información de validación que sea acorde con las restricciones.

3. Método según cualquiera de las reivindicaciones anteriores, en el que la determinación de rutas incluye construir un grafo dirigido de raíces de confianza y el subconjunto de certificados y llevar a cabo una búsqueda acíclica en profundidad del grafo.

4. Método según cualquiera de las reivindicaciones anteriores, en el que las pruebas se almacenan en la tabla que contiene la información de validación.

5. Método según cualquiera de las reivindicaciones anteriores, en el que las pruebas se almacenan en otra tabla que está separada de la tabla que contiene la información de validación.

6. Método según cualquiera de las reivindicaciones anteriores, en el que la tabla se indexa utilizando las raíces de confianza o utilizando los certificados.

7. Método, según la reivindicación 5, en el que la otra tabla se indexa utilizando las raíces de confianza o utilizando los certificados.

8. Método según cualquiera de las reivindicaciones anteriores, en el que el subconjunto de certificados incluye raíces de confianza, autoridades que emiten certificados de usuario final, y autoridades que avalan a otras autoridades.

9. Método según la reivindicación 8, en el que el subconjunto de certificados además incluye certificados de usuario final.

10. Producto de programa de ordenador previsto en unos medios de almacenamiento internos para su ejecución en un procesador, que comprende un código ejecutable para ejecutar las etapas del método según cualquiera de las reivindicaciones anteriores.

11. Servidor (30), que comprende:

un procesador;

unos medios de almacenamiento internos acoplados al procesador;

el producto de programa de ordenador de la reivindicación 10 previsto en los medios de almacenamiento internos.

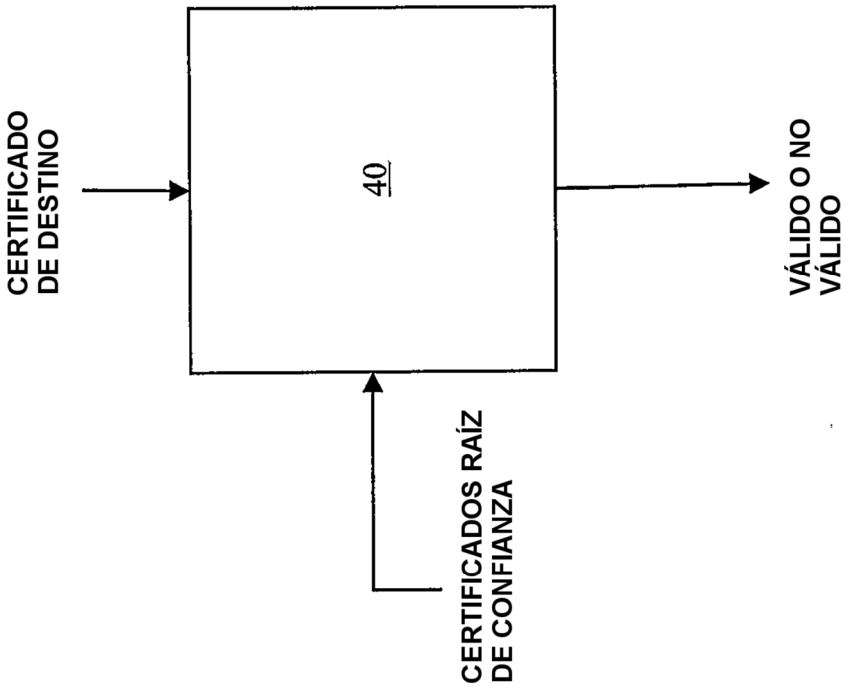

FIGURA 2

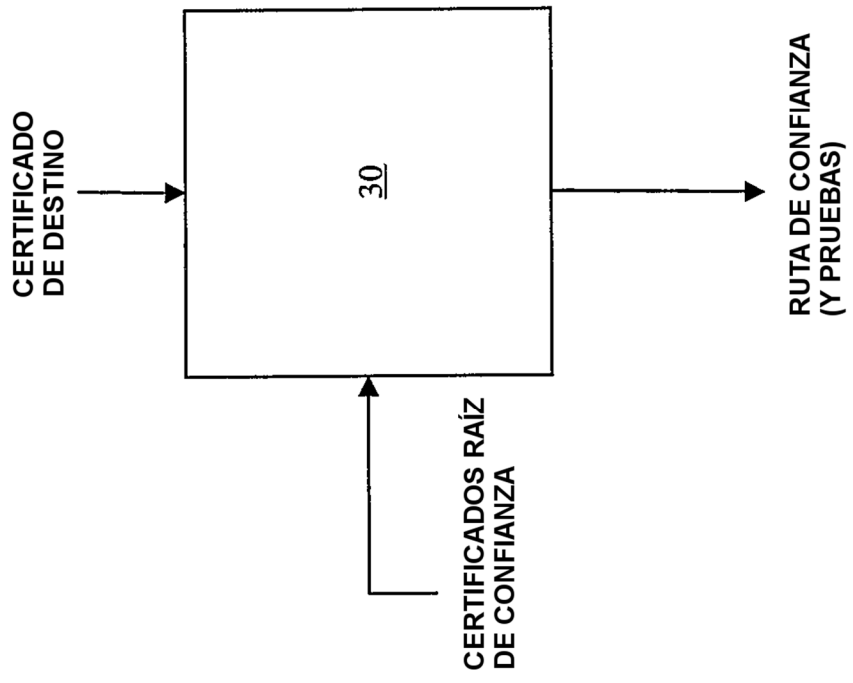

FIGURA 1

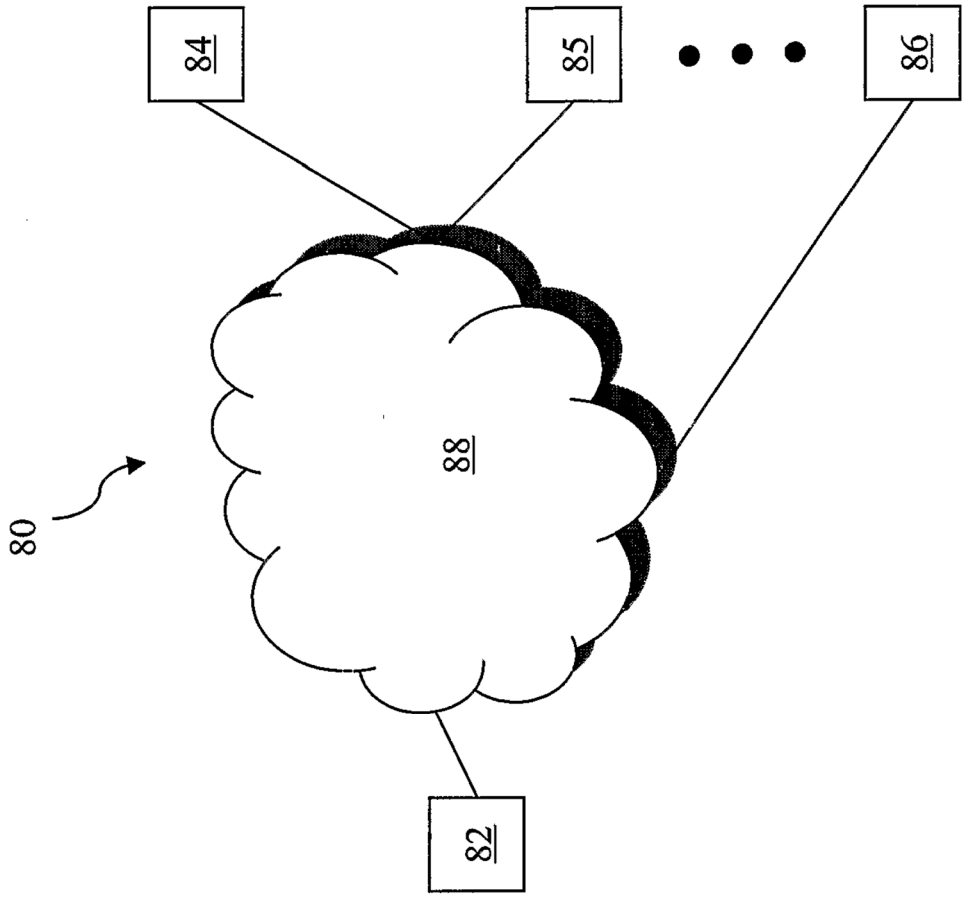

FIGURA 4

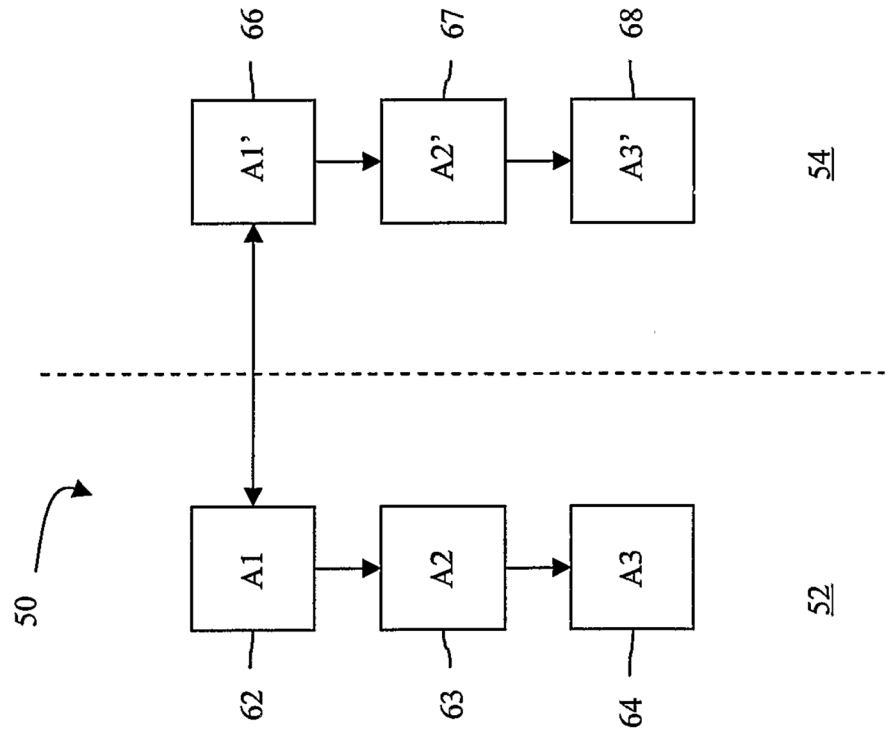

FIGURA 3

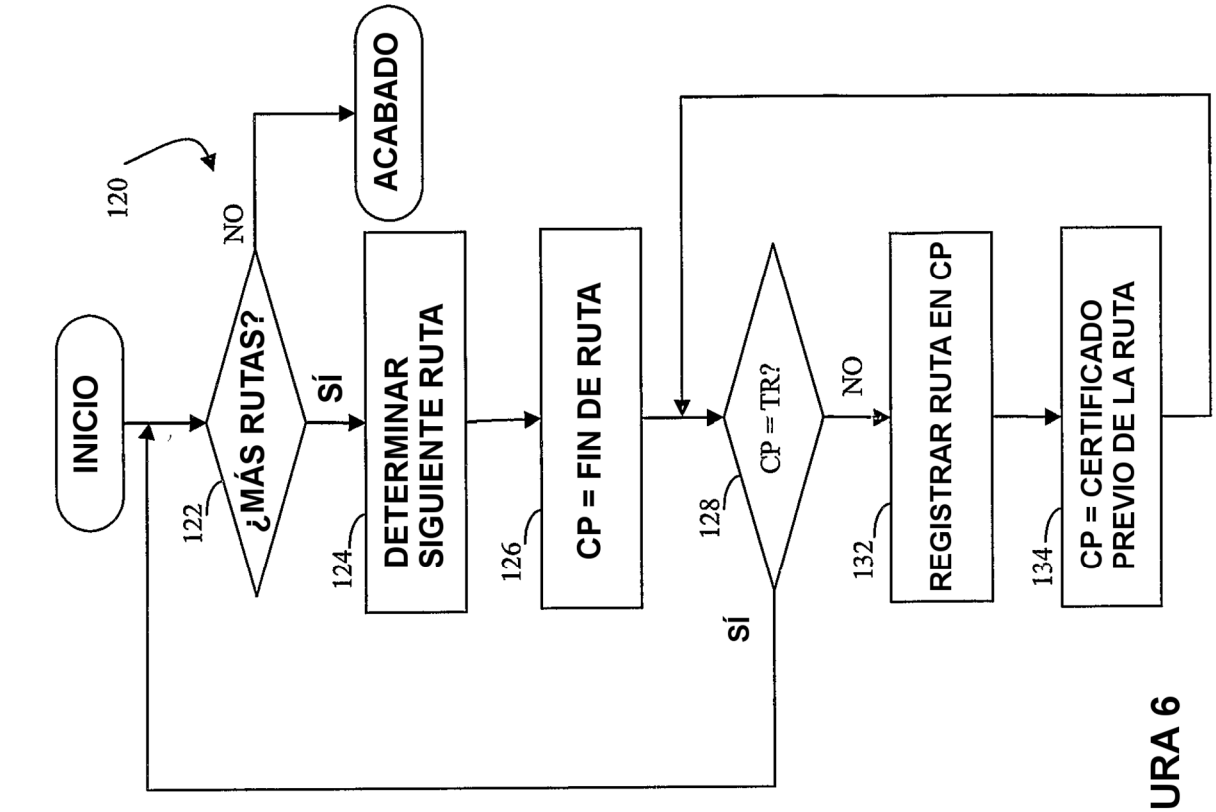

FIGURA 6

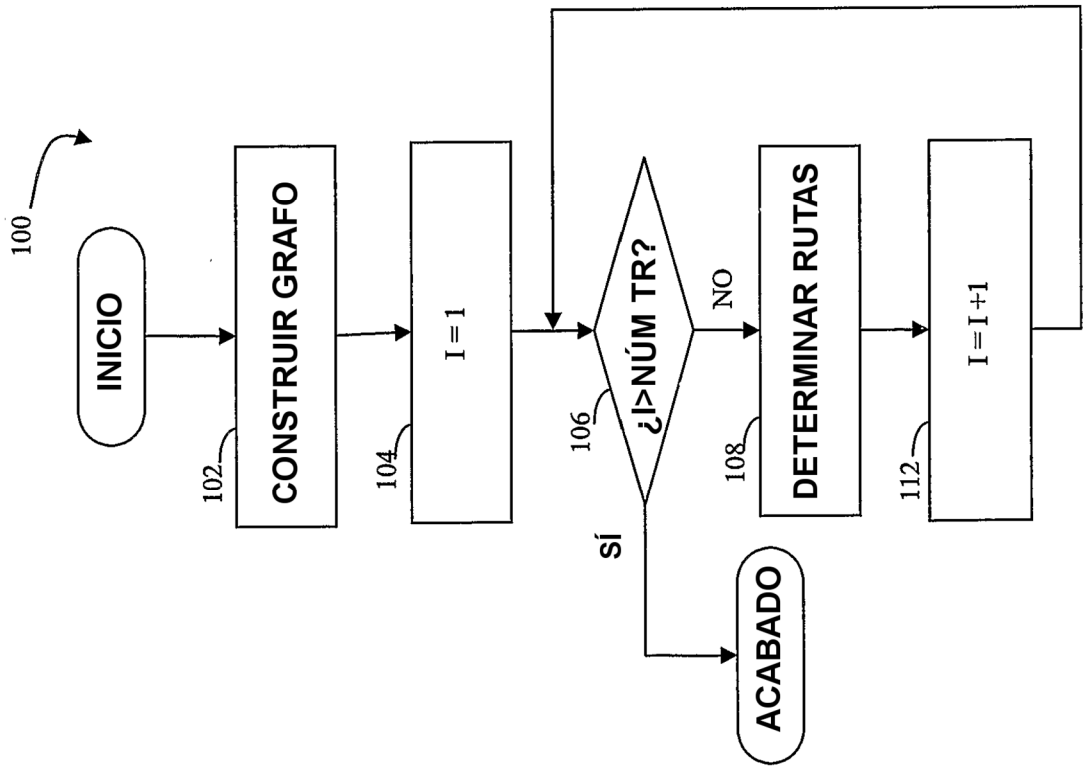

FIGURA 5

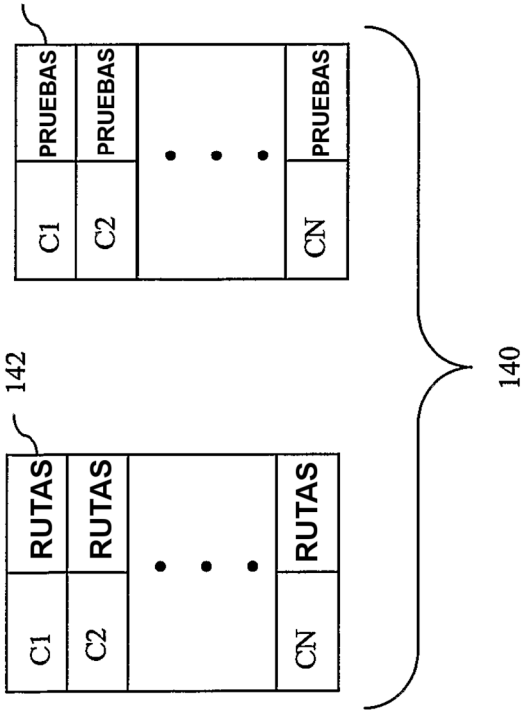

FIGURA 7A

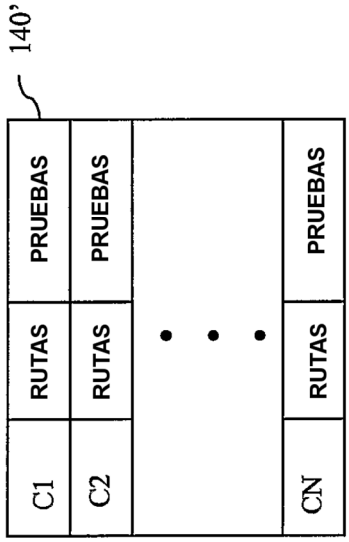

FIGURA 7B

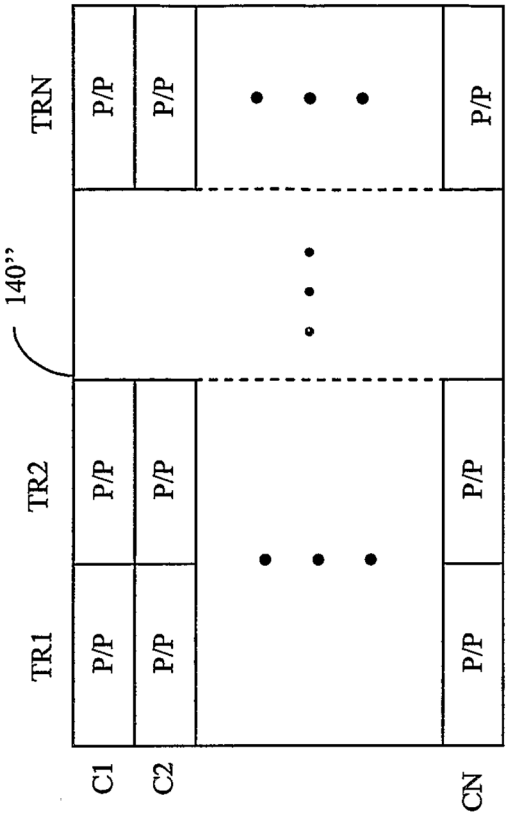

FIGURA 7C

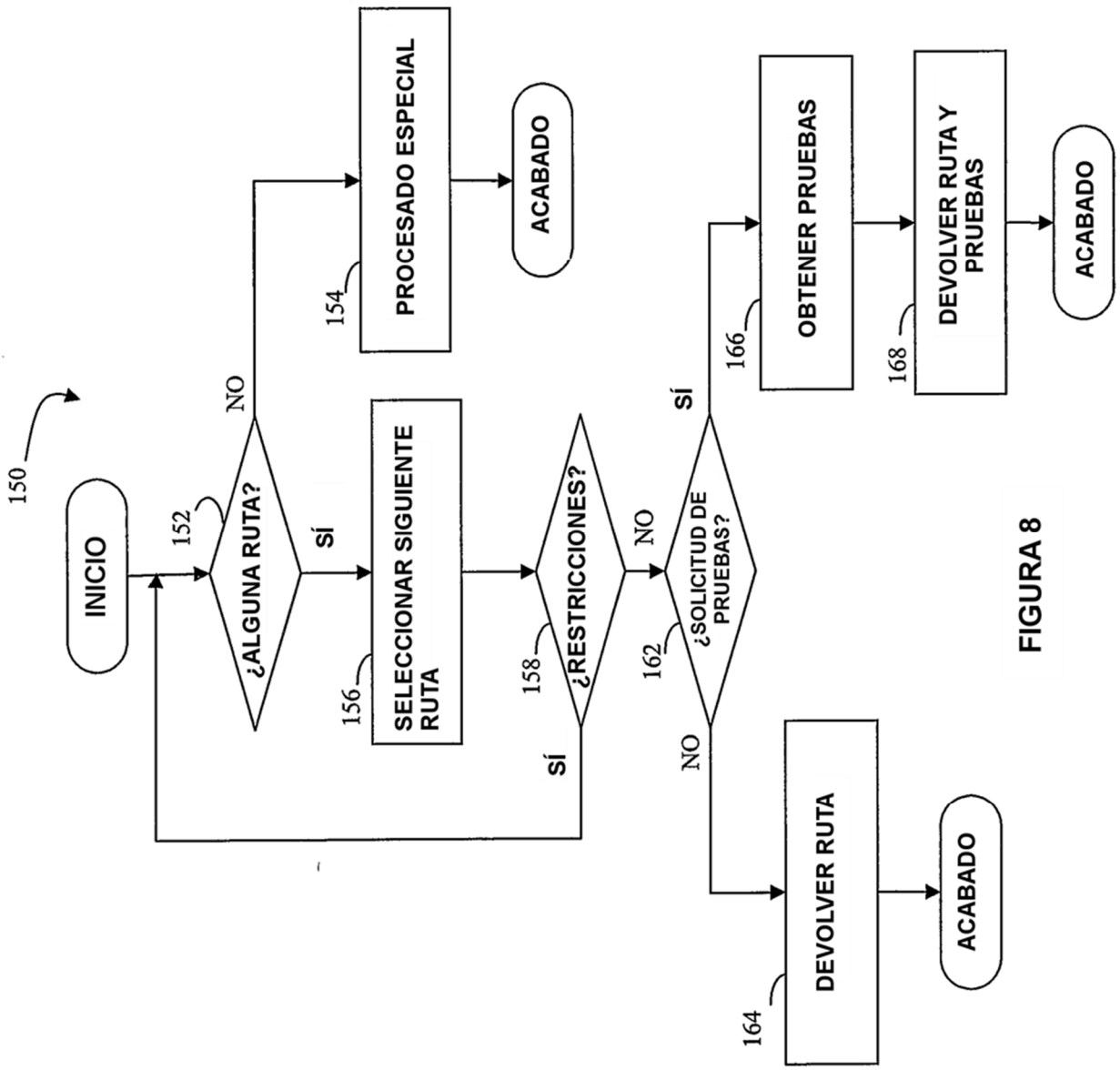
150
INICIO
152
¿ALGUNA RUTA?
NO
SÍ
154
PROCESADO ESPECIAL
ACABADO
156
SELECCIONAR SIGUIENTE RUTA
158
¿RESTRICCIONES?
SÍ
NO
162
¿SOLICITUD DE PRUEBAS?
SÍ
166
OBTENER PRUEBAS
168
DEVOLVER RUTA Y PRUEBAS
ACABADO
NO
164
DEVOLVER RUTA
ACABADO

FIGURA 8

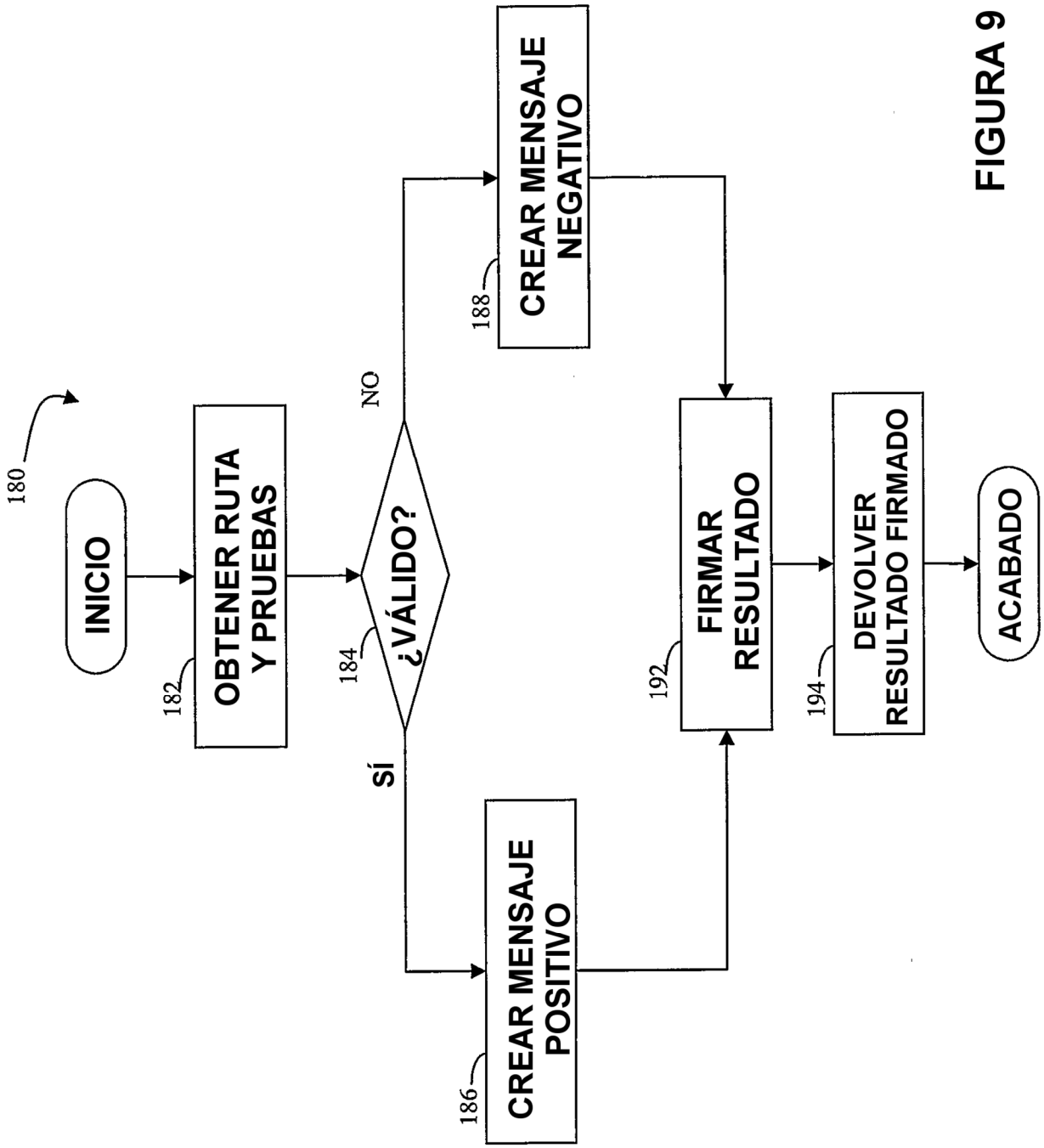
180
INICIO
182
OBTENER RUTA Y PRUEBAS
184
¿VÁLIDO?
NO
SÍ
188
CREAR MENSAJE NEGATIVO
186
CREAR MENSAJE POSITIVO
192
FIRMAR RESULTADO
194
DEVOLVER RESULTADO FIRMADO
ACABADO

FIGURA 9