(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 597 815**

(51) Int. CI.:

G06F 21/33 (2013.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **04.01.2008 PCT/US2008/050204**

(87) Fecha y número de publicación internacional: **24.07.2008 WO08088944**

(96) Fecha de presentación y número de la solicitud europea: **04.01.2008 E 08713521 (6)**

(97) Fecha y número de publicación de la concesión europea: **20.07.2016 EP 2109955**

(54) Título: **Aprovisionamiento de representaciones de identidad digital**

(30) Prioridad:

18.01.2007 US 885598 P
17.09.2007 US 856617

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.01.2017

(73) Titular/es:

MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)
One Microsoft Way
Redmond, WA 98052, US

(72) Inventor/es:

GAJJALA, VIJAY K.;
BRACE, COLIN H.;
DEL CONTE, DEREK T.;
CAMERON, KIM;
NANDA, ARUN K.;
WILSON, HERVEY O.;
KWAN, STUART L.S.;
RAJ, RASHMI y
NORI, VIJAYAVANI

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Aprovisionamiento de representaciones de identidad digital

Antecedentes

Recientemente ha tenido lugar una innovación tremenda en sistemas de desarrollo para proporcionar a los individuos más control sobre cómo se distribuye y usa su información de identidad personal, particularmente en un contexto digital. Por ejemplo, Microsoft Corporation de Redmond, Washington, entre otros, ha propagado un sistema en ocasiones denominado como el Selector de Tarjeta de Información - denominándose la instanciación de Microsoft como Windows CardSpace. En un sistema Windows CardSpace, un principal obtiene una o más representaciones de identidad digital, en ocasiones denominadas como tarjetas de información. Cuando el principal intenta acceder a un recurso (una "parte confiante") que solicita un conjunto de reclamaciones realizadas acerca del principal, el principal emplea una representación de identidad digital (en lo sucesivo denominada una "DIR") para iniciar la comunicación con un proveedor de identidad que puede afirmar estas reclamaciones. En algunos casos, el proveedor de identidad puede controlarse mediante un principal y ejecutarse en la propia máquina del principal. En otros puede controlarse mediante una tercera parte. El proveedor de identidad devuelve un "testigo de identidad" que incluye la información de las reclamaciones requerida.

Se ha dirigido poca atención, sin embargo, hacia la creación y aprovisionamiento de las DIR. Actualmente, los administradores de sistemas de identidad digital se ven forzados a formar las DIR manualmente. Por ejemplo, un administrador puede usar manualmente una utilidad de software, tal como un generador de XML, para formar una DIR y grabarla a una localización particular. El administrador puede a continuación enviar al principal un puntero a la DIR, y el principal iría a continuación a recuperar la DIR. Este sistema es ad hoc, sometido a errores y vulnerabilidades de seguridad, y de trabajo intensivo para un administrador.

El documento US 2005/283443 A1 se refiere a un sistema de gestión de identidad. En un sistema de gestión de identidad jerárquico distribuido, se asigna a los usuarios un identificador único global (GUID) que se denomina también como un identificador personal globalmente único (GUPI). Un sitio de miembros (MS) proporciona al usuario un servicio, y requiere información de identificación acerca del usuario que se obtendrá desde un sitio doméstico (HS). Un usuario emplea un explorador para iniciar una sesión con el MS, y a continuación se le solicita información de identificación o un inicio de sesión. El usuario indica que la información requerida puede proporcionarse mediante el HS. El MS genera una solicitud para la información almacenada mediante el HS y la reenvía, preferentemente como una forma HTTPS, al usuario. La forma HTTPS tiene preferentemente un número aleatorio utilizado sólo una vez asociado con él para actuar como un identificador de sesión e incluye una redirección al HS. Si el usuario todavía no ha iniciado sesión y se ha autenticado, el HS obtiene información de inicio de sesión para autenticar al usuario. El HS a continuación busca preferentemente autorización de usuario para liberar la información solicitada al MS. La información solicitada podría ser tan sencilla como el GUPI proporcionado como un par nombre-valor codificado en URL, o tan rico como un fragmento de XML.

El documento US 2004/162786 A1 se refiere a un procedimiento y dispositivo asociado para gestionar ciclos de vida de ID digital para programas de aplicación, y programas de aplicación de abstracción para múltiples tipos de credenciales a través de un Sistema de Gestión de Identidad Digital (DIMS) común y una capa de Interfaz de Programación de Aplicación (API).

El documento US 2006/005020 A1 se refiere a un procedimiento y sistema para seguridad escalonada en un sistema de gestión de identidad que utiliza diferentes niveles de sensibilidad de tiempo, seguridad de canal y seguridad de autenticación para proporcionar un enfoque multidimensional para proporcionar el ajuste correcto para diferentes solicitudes de identidad. Los diferentes niveles de seguridad pueden seleccionarse mediante preferencias de usuario, solicitud de sitio de miembros o política de sitio doméstico.

Sumario

Es el objeto de la presente invención proporcionar un sistema y procedimiento para aprovisionar una representación de identidad digital (DIR) para un principal.

Este objeto se resuelve mediante la materia objeto de las reivindicaciones independientes.

Se proporcionan realizaciones en las reivindicaciones dependientes.

Este resumen se proporciona para introducir una selección de conceptos en una forma simplificada que se describen adicionalmente a continuación en la descripción detallada. Este resumen no se pretende para identificar características clave o características esenciales de la materia objeto reivindicada, ni se pretende para usarse como un ayuda al determinar el alcance de la materia objeto reivindicada.

Un aspecto se refiere a un sistema para aprovisionar una DIR para un principal. El sistema incluye un sistema de generación de DIR que está adaptado para recibir una solicitud para generar una DIR para el principal y a continuación generar la DIR. También se proporciona un proveedor de identidad adaptado para generar un testigo

de identidad en respuesta a la comunicación iniciada usando la DIR, y un almacenamiento de datos de identidad, conectado de manera operativa tanto al sistema de generación de DIR como al proveedor de identidad. El sistema de generación de DIR accede al almacenamiento de datos de identidad al generar la DIR y el proveedor de identidad también accede al almacenamiento de datos de identidad al generar el testigo de identidad.

Otro aspecto se refiere a un procedimiento para aprovisionar una DIR para un principal. El procedimiento incluye autenticar el principal en un sistema de generación de DIR usando información de inicio de sesión tal como un nombre de usuario y contraseña. El procedimiento incluye adicionalmente recibir una solicitud para una DIR y generar la DIR solicitada de una manera que incluya al menos alguna de la información de inicio de sesión. Por ejemplo, la misma información de inicio de sesión puede usarse para proteger o "respaldar" la DIR resultante. Esto proporciona un indicio para el principal de autenticación con respecto a qué información de autenticación proporcionar en un momento más adelante para iniciar sesión.

Otro aspecto se refiere a otro procedimiento para aprovisionar una DIR para un principal. En este procedimiento ejemplar, se genera un primer descriptor de DIR y un segundo descriptor de DIR. Estos pueden presentar, por ejemplo, diferentes DIR que están disponibles para los principales. A continuación, el primer y segundo descriptores de DIR se envían al principal de modo que el principal conoce, por ejemplo, qué DIR están disponibles. Se recibe a continuación una solicitud desde el principal para al menos una primera DIR conforme al primer descriptor de DIR. La primera DIR se crea a continuación.

Otro aspecto se refiere a otro procedimiento más para aprovisionar una DIR para un principal. Se solicita el acceso a una parte confiante. Se recibe a continuación un mensaje que deniega el acceso y que transmite la política de seguridad de la parte confiante. Una DIR que satisface la política de seguridad se solicita a continuación desde un sistema de generación de DIR. Finalmente, se recibe la DIR.

Breve descripción de los dibujos

Se hará referencia ahora a los dibujos adjuntos, que no están necesariamente dibujados a escala, y en los que:

La Figura 1 ilustra un sistema de DIR de ejemplo que incluye un principal, una máquina principal, una parte confiante, un proveedor de identidad, un sistema de generación de DIR, un almacenamiento de datos de identidad, un sistema de administrador, y un sistema de captura de datos;
La Figura 2 ilustra un procedimiento de ejemplo para aprovisionamiento y uso de DIR;
La Figura 3 ilustra otro procedimiento de ejemplo para aprovisionamiento y uso de DIR;
La Figura 4 ilustra otro procedimiento de ejemplo para aprovisionamiento de DIR;
La Figura 5 ilustra otro procedimiento de ejemplo para aprovisionamiento de DIR;
La Figura 6 ilustra otro procedimiento de ejemplo para aprovisionamiento de DIR;
La Figura 7 ilustra otro procedimiento de ejemplo para aprovisionamiento de DIR;
La Figura 8 ilustra otro procedimiento de ejemplo para aprovisionamiento de DIR; y
La Figura 9 ilustra un ejemplo de un dispositivo informático.

Descripción detallada:

Se describirán ahora realizaciones de ejemplo más completamente en lo sucesivo con referencia a los dibujos adjuntos. Números de referencia similares hacen referencia a elementos similares a lo largo de todo el presente documento.

Las realizaciones de ejemplo desveladas en el presente documento se refiere en general a sistemas de identidad que incluyen DIR usadas al iniciar comunicación para producción de testigos de identidad que pueden intercambiarse entre un principal, un proveedor de identidad, y una parte confiante para autenticar una identidad y/o información relacionada con el principal. En realizaciones de ejemplo del presente documento, el principal puede ser una persona o personas naturales, un ordenador, una red o cualquier otra entidad. La parte confiante tiene bienes, servicios u otra información que el principal desea acceder y/u obtener. En realizaciones de ejemplo, la parte confiante puede ser cualquier recurso, privilegio o servicio que requiere una política de seguridad para entrar, acceso o uso. Por ejemplo, una parte confiante puede comprender uno o más de: ordenadores, redes de ordenadores, datos, bases de datos, edificios, personal, servicios, compañías, organizaciones, localizaciones físicas, dispositivos electrónicos o cualquier otro tipo de recurso.

Haciendo referencia ahora a la Figura 1, se muestra un sistema 100 de DIR de ejemplo que incluye un principal 110 y una parte 120 confiante. El principal 110 está en posesión o control sobre la máquina 111 principal. La máquina 111 principal incluye un sistema informático controlado al menos temporalmente mediante el principal 110. La parte 120 confiante puede incluir también un sistema informático. El sistema 100 puede incluir también un sistema 160 de administrador, un sistema 162 de captura de datos, un sistema 164 de generación de DIR, y almacenamiento 168 de datos de identidad, y un proveedor 115 de identidad, cada uno de los cuales se analiza adicionalmente a continuación y puede incluir, o ser parte de, un sistema informático.

El principal 110 y la parte 120 confiante pueden comunicar entre sí a través de una o más redes, tal como internet, o a través de formas telefónicas u otras de comunicación cableada o inalámbrica. En realizaciones de ejemplo, el

principal 110 puede solicitar bienes, servicios, información, privilegios u otra forma de acceso a partir de la parte 120 confiante. La parte 120 confiante puede requerir autenticación de la identidad de, o información acerca del, principal 110 antes o en conjunto con proporcionar el acceso solicitado al principal 110.

También se muestra en la Figura 1 un proveedor 115 de identidad de ejemplo. El proveedor 115 de identidad incluye un sistema informático. En realizaciones de ejemplo, el proveedor 115 de identidad incluye un transformador 130 de reclamaciones y una autoridad 140 de reclamaciones. El transformador 130 de reclamaciones se denomina en ocasiones como un "servicio de testigo de seguridad". En el ejemplo mostrado, el proveedor 115 de identidad puede proporcionar una o más reclamaciones acerca del principal 110. Una reclamación es una sentencia o afirmación realizada acerca del principal, que incluye posiblemente información acerca del principal tal como, por ejemplo, nombre, dirección, número de la seguridad social, edad, historial de crédito, requisitos transaccionales, etc. Como se describe adicionalmente a continuación, el proveedor 115 de identidad puede proporcionar reclamaciones al principal 110 y/o a la parte 120 confiante en forma de un testigo de identidad firmado digitalmente. En realizaciones de ejemplo, el proveedor 115 de identidad está en una relación confiable con la parte 120 confiante, de modo que la parte 120 confiante confía las reclamaciones en el testigo de identidad firmado desde el proveedor 115 de identidad.

Aunque el transformador 130 de reclamaciones y la autoridad 140 de reclamaciones del proveedor 115 de identidad se muestran como entidades separadas en la Figura 1, en realizaciones alternativas el transformador 130 de reclamaciones y la autoridad 140 de reclamaciones pueden ser la misma entidad o entidades diferentes. El proveedor 115 de identidad puede tomar la forma de un servicio de testigo de seguridad en algunas realizaciones de ejemplo. De manera similar, el proveedor 115 de identidad y el sistema 164 de generación de DIR pueden ser la misma o diferentes entidades.

Los sistemas informáticos descritos en el presente documento incluyen, sin limitación, un ordenador personal, ordenador servidor, dispositivo de mano o portátil, sistema de microprocesador, sistema basado en microprocesador, electrónica de consumo programable, PC de red, miniordenadores, ordenador central, tarjeta inteligente, teléfono, dispositivo de comunicación móvil o celular, asistente de datos personal, entorno informático distribuido que incluye cualquiera de los sistemas o dispositivos anteriores y similares. Algunos sistemas informáticos descritos en el presente documento pueden comprender dispositivos informáticos portátiles. Un dispositivo informático portátil es cualquier sistema informático que está diseñado para llevarse físicamente por un usuario. Cada sistema informático puede incluir también uno o más periféricos, incluyendo sin limitación: teclado, ratón, una cámara, una cámara web, una cámara de vídeo, un escáner de huellas digitales, un escáner de iris, un dispositivo de visualización tal como un monitor, un micrófono o altavoces.

Cada sistema informático incluye un sistema operativo, tal como (sin limitación) el sistema operativo WINDOWS de Microsoft Corporation, y uno o más programas almacenados en el medio legible por ordenador. Cada sistema informático puede incluir también uno o más dispositivos de comunicaciones de entrada y salida que permiten al usuario comunicar con el sistema informático, así como permitir al sistema informático comunicar con otros dispositivos. Las comunicaciones entre los sistemas informáticos usados mediante el principal 110 (por ejemplo, máquina 111 principal), parte 120 confiante, sistema 164 de generación de DIR, sistema 160 de administrador, sistema 162 de captura de datos, y proveedor 115 de identidad pueden implementarse usando cualquier tipo de enlace de comunicaciones, incluyendo, sin limitación, internet, redes de área extensa, intranets, Ethernet, rutas cableadas directas, satélites, escáneres de infrarrojos, comunicaciones celulares o cualquier otro tipo de comunicaciones cableadas o inalámbricas.

En algunas realizaciones de ejemplo desveladas en el presente documento, el sistema 100 se implementa al menos en parte como un sistema de tarjeta de información proporcionado en la estructura .NET 3.0 desarrollada por Microsoft Corporation de Redmond, Washington. El sistema de tarjeta de información permite a los principales manejar múltiples DIR desde diversos proveedores de identidad.

El sistema de tarjeta de información utiliza una plataforma de servicios web tal como la Estructura de Comunicación de Windows en la estructura .NET 3.0. Además, el sistema de tarjeta de información se crea usando las especificaciones de seguridad de servicios web propagadas al menos en parte por Microsoft Corporation de Redmond, Washington. Estas especificaciones incluyen un modelo de seguridad de mensaje seguridad WS, una política de seguridad WS de política de punto de extremo, un intercambio de metadatos WS, y un modelo de confianza WS-Tmst. En general, el modelo de seguridad WS describe cómo unir testigos de identidad a mensajes. El modelo de política de seguridad WS describe requisitos de política de punto de extremo, tales como testigos de identidad requeridos y algoritmos de encriptación soportados. Tales requisitos de política pueden transportarse y negociarse usando un protocolo de metadatos definido mediante intercambio de metadatos WS. El modelo de confianza WS describe una estructura para modelos de confianza que posibilita que interoperen diferentes servicios web. Algunas realizaciones de ejemplo descritas en el presente documento hacen referencia a las especificaciones de seguridad de servicios web anteriormente descritas. En realizaciones alternativas, una u otras especificaciones más pueden usarse para facilitar las comunicaciones entre los diversos subsistemas en el sistema 100.

Haciendo referencia de nuevo a la Figura 1, el principal 110 puede enviar una solicitud mediante la máquina 111 principal a la parte 120 confiante para acceder a bienes, servicios, u otra información. Por ejemplo, en una realización, la máquina 111 principal envía una solicitud a la parte 120 confiante para acceder a información desde la

parte 120 confiante que el principal 110 desea. La solicitud enviada mediante la máquina 111 principal puede incluir una solicitud para los requisitos de autenticación de la parte 120 confiante usando, por ejemplo, los mecanismos proporcionados en intercambio de metadatos WS.

En respuesta a la solicitud, la parte 120 confiante puede enviar a la máquina 111 principal requisitos para que la parte 120 confiante autentique la identidad del principal u otra información acerca del principal 110. Los requisitos de la parte 120 confiante para autenticación se denominan en el presente documento como una política de seguridad. Una política de seguridad define mínimamente el conjunto de reclamaciones desde un proveedor 115 de identidad confiable que el principal 110 debe proporcionar a la parte 120 confiante para que la parte 120 confiante autentique al principal 110. Una política de seguridad puede incluir un requisito de prueba con respecto a una característica personal (tal como edad), identidad, estado financiero, etc. Puede incluir también reglas con respecto al nivel de verificación y autenticación requeridas para autenticar cualquier oferta de prueba (por ejemplo, firma digital desde un proveedor de identidad particular).

En un ejemplo, la parte 120 confiante especifica su política de seguridad usando política de seguridad WS, incluyendo tanto los requisitos de reclamación como el tipo de testigo de identidad requeridos por la parte 120 confiante. Ejemplos de tipos de reclamaciones incluyen, sin limitación, los siguientes: nombre, apellidos, dirección de correo electrónico, dirección de la calle, nombre de localidad o ciudad, estado o provincia, código postal, país, número de teléfono, número de la seguridad social, fecha de nacimiento, género, número de identificador personal, calificación de crédito, estado financiero, estado legal, etc.

La política de seguridad puede usarse también para especificar el tipo de testigo de identidad requerido por la parte 120 confiante, o puede usarse un tipo por defecto según se determina por el proveedor de identidad. Además de especificar las reclamaciones requeridas y el tipo de testigo, la política de seguridad puede especificar un proveedor de identidad particular requerido por la parte confiante. Como alternativa, la política puede omitir este elemento, dejando la determinación del proveedor de identidad apropiado al principal 110. Pueden especificarse también otros elementos en la política de seguridad tales como, por ejemplo, la caducidad del testigo de seguridad requerida.

En algunas realizaciones, el principal 110 puede requerir que la parte 120 confiante se identifique así misma a la máquina 111 principal de modo que el principal 110 pueda decidir si satisfacer o no la política de seguridad de la parte 120 confiante, como se describe más adelante. En un ejemplo, la parte 120 confiante se identifica así misma usando un certificado X509. En otras realizaciones, la parte 120 confiante puede identificarse a sí misma usando otros mecanismos tales como, por ejemplo, un certificado de servidor de Capa de Conexiones Seguras ("SSL").

La máquina 111 principal puede incluir una o más DIR para el principal 110. Estas DIR (en ocasiones denominadas como "tarjetas de información" en el sistema de Windows Cardspace proporcionado en la estructura .NET 3.0 desarrollada por Microsoft Corporation de Redmond, Washington) son artefactos que representan la relación de emisión de testigo entre el principal 110 y un proveedor de identidad particular, tal como el proveedor 115 de identidad. Cada DIR puede corresponder a un proveedor de identidad particular, y el principal 110 puede tener múltiples DIR a partir del mismo o diferentes proveedores de identidad. El uso de las DIR en un sistema de identidad se describe en detalle en la Solicitud de Patente de Estados Unidos N. º 11/361.281.

Las DIR pueden incluir, entre otra información, la política de emisión del proveedor de identidad para testigos de identidad, incluyendo el tipo de testigos que pueden emitirse, los tipos de reclamaciones para los que tiene autoridad, y/o las credenciales para usar para la autenticación cuando se solicitan testigos de identidad. Las DIR pueden representarse como documentos de XML que se emiten por los proveedores 115 de identidad o los sistemas 164 de generación de DIR y almacenarse mediante los principales 110 en un dispositivo de almacenamiento tal como la máquina 111 principal.

La máquina 111 principal puede incluir también un selector de identidad. En general, un selector de identidad es un programa informático e interfaz de usuario que permiten al principal 110 seleccionar entre una o más DIR del principal 110 en la máquina 111 principal para solicitar y obtener testigos de identidad desde uno o más proveedores de identidad, tal como el proveedor 115 de identidad. Por ejemplo, cuando se recibe una política de seguridad desde la parte 120 confiante mediante la máquina 111 principal, el selector de identidad puede programarse para identificar una o más DIR que satisfacen una o más de las reclamaciones requeridas por la política de seguridad usando la información en las DIR. Una vez que el principal 110 recibe la política de seguridad desde la parte 120 confiante, el principal 110 puede comunicar con (usando, por ejemplo, la máquina 111 principal) uno o más proveedores de identidad para recoger las reclamaciones requeridas por la política.

En realizaciones de ejemplo, el principal 110 solicita uno más testigos de identidad desde el proveedor 115 de identidad usando el mecanismo de emisión descrito en confianza WS. En realizaciones de ejemplo, el principal 110 reenvía los requisitos de reclamación en la política de la parte 120 confiante al proveedor 115 de identidad. La identidad de la parte 120 confiante puede especificarse, pero no es necesario, en la solicitud enviada mediante el principal 110 al proveedor 115 de identidad. La solicitud puede incluir otros requisitos también, tal como una solicitud para un testigo de visualización.

En general, la autoridad 140 de reclamaciones del proveedor 115 de identidad puede proporcionar una o más de las reclamaciones requeridas por la política de seguridad desde la parte 120 confiante. El transformador 130 de reclamaciones del proveedor 115 de identidad está programado para transformar las reclamaciones y para generar uno o más testigos 150 de identidad firmados que incluyen la reclamación o reclamaciones relacionadas con el principal 110.

Como se ha indicado anteriormente, el principal 110 puede solicitar un testigo de identidad en un cierto formato en su solicitud al proveedor 115 de identidad, basándose en requisitos desde la parte 120 confiante. El transformador 130 de reclamaciones puede programarse para generar testigos de identidad en uno de una pluralidad de formatos incluyendo, sin limitación, X509, Kerberos, SAML (versiones 1.0 y 2.0), Protocolo de identidad sencillo extensible ("SXIP"), etc.

Por ejemplo, en una realización, la autoridad 140 de reclamaciones está programada para generar reclamaciones en un primer formato A, y la política de seguridad de la parte 120 confiante requiere un testigo de identidad en un segundo formato B. El transformador 130 de reclamaciones puede transformar las reclamaciones de la autoridad 140 de reclamaciones desde el formato A en el formato B antes de enviar un testigo de identidad al principal 110. Además, el transformador 130 de reclamaciones puede programarse para perfeccionar la semántica de una reclamación particular. En realizaciones de ejemplo, la semántica de una reclamación particular se transforma para minimizar la cantidad de información proporcionada en una reclamación particular y/o testigo de identidad para reducir o minimizar la cantidad de información personal que se transporta mediante una reclamación dada.

En realizaciones de ejemplo, el transformador 130 de reclamaciones reenvía el testigo 150 de identidad al principal 110 usando los mecanismos de respuesta descritos en confianza WS. En una realización, el transformador 130 de reclamaciones incluye un servicio de testigo de seguridad (en ocasiones denominado como un "STS"). En una realización de ejemplo, el principal 110 reenvía el testigo 150 de identidad a la parte 120 confiante vinculando el testigo 150 de identidad a un mensaje de aplicación usando los mecanismos de vinculación de seguridad descritos en seguridad WS. En otras realizaciones, el testigo 150 de identidad puede enviarse directamente desde el proveedor 115 de identidad a la parte 120 confiante.

Una vez que la parte 120 confiante recibe el testigo 150 de identidad, la parte 120 confiante puede verificar (por ejemplo, decodificando o desencriptando el testigo 150 de identidad) el origen del testigo 150 de identidad firmado. La parte 120 confiante puede utilizar también la reclamación o reclamaciones en el testigo 150 de identidad para satisfacer la política de seguridad de la parte 120 confiante para autenticar el principal 110.

El aprovisionamiento de las DIR se analizará ahora en mayor detalle. El principal 110 puede obtener una DIR de una diversidad de maneras. En la realización de ejemplo ilustrada en la Figura 1, el sistema 164 de generación de DIR se usa en general para comunicar con el principal 110, crear nuevas DIR, y notificar al principal 110 de DIR disponibles. El sistema 164 de generación de DIR puede comprender en algunas realizaciones un sitio web de internet. En otras realizaciones, el sistema 164 de generación de DIR puede comprender un servicio web. El sistema 164 de generación de DIR puede incluir también o funcionar en conjunto con un servidor 166 de información de internet (IIS) en ciertas realizaciones.

El almacenamiento 168 de datos de identidad es un almacenamiento de información digital que puede accederse en ciertas realizaciones mediante el proveedor 115 de identidad, el sistema 164 de generación de DIR y el sistema 160 de administrador. El almacenamiento 168 de datos de identidad puede comprender un servidor de base de datos, memoria informática o cualquier otro dispositivo o dispositivos de almacenamiento de datos. El almacenamiento 168 de datos de identidad puede estar comprendido de una pluralidad de dispositivos o sistemas en un modelo de datos distribuido. El almacenamiento 168 de datos de identidad puede incluir o comprender un servicio de directorio tal como el Directorio 169 Activo propagado por Microsoft Corporation de Redmond, Washington.

El sistema 160 de administrador puede incluir un sistema informático, que incluye una interfaz de usuario que permitirá a un administrador comunicar con el almacenamiento 168 de datos de identidad y el sistema 164 de generación de DIR. El sistema 160 de administrador permite a un administrador organizar y administrar los datos en el almacenamiento 168 de datos de identidad. Permite también a un administrador determinar los tipos de DIR que el sistema 164 de generación de DIR crea, y permite a un administrador controlar si un principal particular es elegible para recibir DIR particulares. El uso del sistema 160 de administrador se analiza adicionalmente a continuación.

Ciertas realizaciones pueden incluir un sistema 162 de captura de datos separado. El sistema 162 de captura de datos puede comprender un sistema informático adaptado para capturar información relacionada con los principales. Por ejemplo, el sistema 162 de captura de datos puede comprender un sistema informático de recursos humanos que captura información personal acerca de un principal, tal como el nombre, número de teléfono, número de la seguridad social, dirección, etc. El sistema 162 de captura de datos puede incluir almacenamiento separado o puede utilizar el almacenamiento 168 de datos de identidad.

La Figura 2 ilustra un procedimiento 200 que puede implementarse mediante el sistema 100. En la etapa 210, un administrador configura un almacenamiento de datos de identidad. Por ejemplo, un administrador puede usar el sistema 160 de administrador para configurar el almacenamiento 168 de datos de identidad. El administrador puede,

en algunas realizaciones, usar el sistema 160 de administrador para establecer tablas en el almacenamiento 168 de datos de identidad que se usarán para administrar, generar y gestionar las DIR. En una realización ejemplar, el administrador puede determinar los tipos de reclamaciones que se soportarán en las DIR creadas mediante el sistema 164 de generación de DIR y testigos de identidad generados mediante el proveedor 115 de identidad. El administrador puede usar también el sistema 160 de administrador para configurar el almacenamiento 168 de datos de identidad para almacenar información de política, tal como los tipos de testigos que el proveedor 115 de identidad soporta, información de permisos y metadatos de federación. Otra información en el almacenamiento 168 de datos de identidad que puede embeberse en una DIR incluye una fotografía del principal 110 e información de conectividad relacionada con los proveedores de identidad tales como el proveedor 115 de identidad.

El procedimiento 200 a continuación continúa a la etapa 220, cuando el principal 110 solicita una DIR. Una solicitud para una DIR puede hacerse de una diversidad de maneras. Por ejemplo, el principal 110 puede usar la máquina 111 principal para acceder al sistema 164 de generación de DIR. En algunas realizaciones, el sistema 164 de generación de DIR es un sitio web, y la máquina 111 principal accede al sistema 164 de generación de DIR a través de un explorador de internet para solicitar una DIR. En algunas realizaciones, el principal 110 solicita una DIR particular. En otras realizaciones, analizadas adicionalmente a continuación, el principal 110 solicita una lista de DIR disponibles para el principal 110 y elige desde esa lista.

El procedimiento 200 a continuación continúa a la etapa 230, cuando el sistema 164 de generación de DIR comprueba con el almacenamiento 168 de datos de identidad, genera la DIR, y proporciona la DIR al principal 110. En una realización, el sistema 164 de generación de DIR comprueba en primer lugar con el almacenamiento 168 de datos de identidad para determinar si el principal 110 tiene permisos para la DIR solicitada. Esto puede conseguirse de una diversidad de maneras, incluyendo comprobando una DLL de permisos en el almacenamiento 168 de datos de identidad, realizar una comprobación de acceso de Directorio Activo, etc. El sistema 164 de generación de DIR puede acceder también a metadatos de sistema de identidad almacenados en el almacenamiento 168 de datos de identidad para determinar qué tipos de reclamaciones de identidad están disponibles para incluirse en la nueva DIR.

Cuando el sistema 164 de generación de DIR crea la nueva DIR, la DIR puede tomar la forma de un documento de XML y puede incluir, entre otra información: una imagen para visualizar en la máquina principal; una lista de reclamaciones incluidas en la DIR; una lista de tipos de testigo disponibles para la DIR; un identificador de DIR único; un indicio de credencial (analizado adicionalmente a continuación); identificación del proveedor de identidad; y una referencia de punto de extremo para el proveedor 115 de identidad. La nueva DIR puede proporcionarse al principal en una diversidad de maneras también, incluyendo un correo electrónico de la nueva DIR, un mensaje de HTTP u otros procedimientos. Como se usa en el presente documento, "correo electrónico" incluye mensajería de texto, mensajería instantánea y formas similares de comunicación electrónica.

Tras la recepción de la nueva DIR, el principal 110 almacena 240 la DIR, por ejemplo en memoria asociada con la máquina 111 principal. El principal 250 a continuación solicita acceso a una parte confiante, tal como la parte 120 confiante. La parte confiante deniega el acceso (por ejemplo, mediante una redirección a una página de autenticación) y proporciona 260 su política de seguridad de vuelta al principal 110. El principal 110 a continuación selecciona 270 una DIR para satisfacer la política de seguridad de la parte 120 confiante. Esto puede conseguirse, por ejemplo, a través de una interfaz de usuario en la máquina 111 principal que visualiza todas las DIR disponibles para el principal 110. En algunas realizaciones, las DIR que cumplen los requisitos de la política de seguridad de la parte confiante pueden destacarse para el principal 110, y pueden atenuarse otras tarjetas para realizar el procedimiento de selección más fácil para el principal 110.

El principal 110 a continuación envía 280 la solicitud para un testigo de identidad a un proveedor de identidad, tal como el proveedor 115 de identidad. Esta solicitud para un testigo de identidad puede generarse automáticamente mediante la máquina 111 principal tras la selección mediante el principal 110 de una DIR almacenada en la máquina 111 principal. El proveedor 115 de identidad comprueba 285 el almacenamiento 168 de datos de identidad para obtener la información requerida para rellenar el testigo de identidad solicitado. Esta información podría incluir, por ejemplo, datos de reclamaciones. Por ejemplo, si la DIR seleccionada indica una reclamación de edad, el proveedor 115 de identidad puede comprobar el almacenamiento 168 de datos de identidad para determinar la edad del principal 110. El proveedor 115 de identidad a continuación puede crear 285 el testigo de identidad solicitado y enviarlo 290 al principal. El principal a continuación envía 295 el testigo de identidad a la parte confiante y se le concede acceso como se ha analizado anteriormente.

Al proporcionar acceso mediante el proveedor 115 de identidad al mismo almacenamiento 168 de datos de identidad usado mediante el sistema 164 de generación de DIR, un administrador puede asegurar que la generación de las DIR permanece en sincronización con los datos reales disponibles para satisfacer reclamaciones en un testigo de identidad solicitado. Por ejemplo, si un administrador configura el almacenamiento 168 de datos de identidad de manera que los datos para una reclamación de edad no se almacenan allí, a continuación el sistema 164 de generación de DIR no creará una DIR que incluya una opción para una reclamación de edad. De otra manera, pueden surgir problemas de sincronización. Por ejemplo, suponiendo que un administrador crea una nueva DIR ad hoc (sin referencia a datos de identidad disponibles), y se incluye una reclamación de edad y se envía como parte de un respaldo de DIR a un principal. Cuando el principal intenta obtener un testigo de identidad con una reclamación de edad, esa información no está disponible, y el testigo se rechazará por la parte confiante como insuficiente. El

sistema 100, en contraste, permite la sincronización automática de las DIR generadas y la disponibilidad de datos subyacentes para rellenar testigos de identidad correspondientes. Se proporciona a un administrador la capacidad a través del sistema 160 de administrador para hacer cambios en el almacenamiento de datos de identidad que afectarán automáticamente tanto el aprovisionamiento de las DIR como la emisión de correspondientes testigos de identidad.

En algunas realizaciones, cuando el administrador hace cambios particulares al almacenamiento 168 de datos de identidad que afectan a la validez de DIR ya emitidas, cualquier principal que haya recibido DIR afectadas se notifica y permite obtener nuevas DIR. Por ejemplo, suponiendo que las normativas de privacidad requieren que el administrador elimine las direcciones domésticas de cualquier principal almacenadas en el almacenamiento 168 de datos de identidad. Cualquier principal 110 que haya recibido una DIR que incluya una reclamación en cuanto a su dirección doméstica ahora tiene una DIR inválida (puesto que ya no hay ningún dato en el almacenamiento 168 de datos de identidad para satisfacer esa reclamación). En una realización, se notifica a todos tales principales, por ejemplo mediante un correo electrónico desde el sistema 164 de generación de DIR, que la o las DIR son ahora invalidas e invita a los principales a obtener una nueva DIR que no incluya la reivindicación de dirección doméstica ya no soportada más. De esta manera, el cambio sencillo por el administrador al almacenamiento 168 de datos de identidad (a) evita que se emitan nuevas DIR con una reclamación de dirección doméstica, y (b) alerta a los principales que las DIR existentes que incluyen esa reclamación son inválidas y pueden sustituirse.

Haciendo referencia ahora a la Figura 3, se describe un procedimiento 300 ejemplar en relación con el sistema 100 mostrado en la Figura 1. En este ejemplo, el principal 110 autentica a la máquina 111 principal. La máquina 111 principal, por ejemplo, puede estar conectada a una intranet que incluye un servicio de directorio, tal como el servidor 169 de Directorio Activo. La autenticación del principal 110 a la máquina 111 principal puede incluir usar información de inicio de sesión a partir de cualquier procedimiento conocido, incluyendo nombre de usuario/contraseña, tarjeta inteligente, etc. El principal 110 a continuación inicia 320 una solicitud de DIR apuntando, por ejemplo, en un explorador en la máquina 111 principal a un sitio web que comprende el sistema 164 de generación de DIR. El principal 110 a continuación autentica 330 en el sistema 164 de generación de DIR. En algunas realizaciones, la máquina 111 principal, el sistema 164 de generación de DIR, el almacenamiento 168 de datos de identidad, el proveedor 115 de identidad, y el sistema 160 de administrador podrían ser parte de la misma intranet. En esa realización, es posible que pueda estar disponible esa capacidad de inicio de sesión único. Por ejemplo, si la máquina principal está ejecutando un sistema operativo WINDOWS disponible a partir de Microsoft Corporation de Redmond, Washington, y la Autenticación Integrada de Windows está activada, entonces la autenticación en el sistema 164 de generación de DIR puede ser automática e ininterrumpida para el principal 110 - la información usada para iniciar sesión en la máquina 111 principal se pasa al sistema 164 de generación de DIR junto con la solicitud para acceso. En otras realizaciones, el administrador puede configurar el sistema 164 de generación de DIR para requerir una autenticación separada del principal 110. El administrador puede configurar el sistema 164 de generación de DIR para requerir cualquiera de una diversidad de mecanismos de autenticación, incluyendo nombre de usuario/contraseña, tarjeta inteligente, etc. En algunas realizaciones, el principal 110 puede autenticarse mediante el IIS 166, que puede configurarse fácilmente por un administrador para aceptar cualquiera de una diversidad de procedimientos de autenticación.

Una vez que el principal 110 está autenticado, el sistema 164 de generación de DIR accede 350 al almacenamiento 168 de datos de identidad. En este ejemplo, el sistema 164 de generación de DIR toma la forma de un servicio web para permitir la negociación entre el sistema de generación de DIR y el principal 110. En este ejemplo, la negociación determina el tipo de DIR que se devolverá al principal 110. En este caso, el sistema 164 de generación de DIR obtiene 350 descriptores de DIR disponibles. En realizaciones ejemplares, un administrador usa el sistema 160 de administrador para crear descriptores de DIR. Por ejemplo, un administrador TI corporativo puede crear descriptores que representan diferentes DIR para diferentes niveles de empleados. Un empleado a tiempo parcial, por ejemplo, puede tener un conjunto diferente de reclamaciones que un empleado a tiempo completo. Un director general puede tener un conjunto diferente de reclamaciones que un empleado de plantilla. Incluso las imágenes que están asociadas con cada descriptor de DIR pueden variar - por ejemplo, la imagen de DIR del grupo de ventas puede ser naranja mientras que la imagen de la DIR de grupo de contabilidad ser verde. Además, es posible personalizar la imagen de la tarjeta para contener la imagen del principal 110 (obtenida a partir del almacenamiento 168 de datos de identidad). Esto potencia la asociación que el principal 110 hace entre sus DIR y el proveedor 115 de identidad. Proporciona mejores capacidades de "huella digital" también.

En algunas realizaciones, el sistema 160 de administrador incluye una interfaz de usuario que analiza a través de todos los tipos disponibles de información disponible en el almacenamiento 168 de datos de identidad y presenta al administrador con una manera fácil de crear descriptores. Por ejemplo, el administrador puede presentarse con una lista de: (a) clases de principales (por ejemplo, empleado a tiempo parcial, empleado a tiempo completo, miembro de equipo ejecutivo, miembro de grupo de ventas, etc.); (b) tipos de reclamación (nombre, dirección, número de teléfono, edad, etc.); (c) acreditaciones de seguridad; (d) estado de empleado (actual, terminado); etc. El administrador podría a continuación decidir crear distintos descriptores disponibles para algunas o todas las clases de principales. Por ejemplo, todos los principales pueden ser elegibles para recibir una DIR básica que incluya el nombre, número de teléfono y estado de empleado del principal. Sin embargo, únicamente el equipo ejecutivo puede ser elegible para recibir una DIR que incluya también una acreditación de seguridad de alto nivel. Estos descriptores pueden crearse por el administrador y grabarse en el almacenamiento de datos de identidad junto con una política

que delimita a qué principales se permite recibir DIR que corresponden a descriptores particulares. Posibles comandos que pueden ser útiles para un administrador al gestionar descriptores incluyen: "OBTENER DESCRIPTORES, OBTENER TODOS LOS DESCRIPTORES, AÑADIR DESCRIPTORES, CAMBIAR DESCRIPTORES, BORRAR DESCRIPTORES, COPIAR DESCRIPTOR, etc."

La solicitud por el principal 110 para descriptores disponibles puede conseguirse mediante la máquina 111 principal a través de un procedimiento de servicio web tal como "OBTENER DESCRIPTORES". Esto provocaría que el sistema de generación de DIR compruebe el principal 110 contra la política establecida por el administrador para determinar cuáles descriptores, si los hubiera, están disponibles para ese principal 110. Esto puede conseguirse, por ejemplo, mediante una comprobación de acceso de Directorio Activo. Los descriptores pueden almacenarse en cualquiera o todos de, por ejemplo: un almacenamiento 168 de datos de identidad, memoria asociada con el sistema 164 de generación de DIR o un almacenamiento separado.

El sistema 164 de generación de DIR a continuación envía 360 los descriptores disponibles a la máquina 111 principal. El principal 110 a continuación selecciona 370 desde los descriptores disponibles y solicita la o las DIR particulares que corresponden al descriptor o descriptores. De nuevo, esto puede conseguirse, por ejemplo, mediante un procedimiento de servicio web tal como "OBTENER TARJETA O TARJETAS" (que hace referencia en este ejemplo a tarjetas de información disponibles en el sistema Windows CardSpace propagado al menos en parte por Microsoft Corporation de Redmond, Washington). Un principal 110 puede solicitar una o varias DIR disponibles.

El sistema 164 de generación de DIR a continuación crea 380 la o las DIR solicitadas. En realizaciones ejemplares, el sistema de generación de DIR incluye en la DIR un indicio de credencial para "respaldar" la DIR. Por ejemplo, la DIR puede incluir un indicio de credencial de nombre de usuario/contraseña, y el principal 110 puede requerirse que autentique usando ese nombre de usuario/contraseña para usar la DIR para obtener un testigo de identidad. En algunas realizaciones, el tipo de autenticación puede tomarse a partir de la autenticación usada mediante el principal 110 para obtener acceso al sistema 164 de generación de DIR. Por ejemplo, si el principal 110 usó una combinación de nombre de usuario/ contraseña para autenticarse al IIS 166, el sistema 164 de generación de DIR puede usar el mismo nombre de usuario y contraseña para respaldar la DIR cuando se envía de vuelta al principal 110.

En otras realizaciones, el sistema de generación digital puede tener acceso a un servicio de directorio, tal como el Directorio 169 Activo, que puede incluir otros procedimientos de autenticación disponibles para un principal 110 particular. Por ejemplo, si el principal 110 usa un nombre de usuario/contraseña para autenticar al sistema 164 de generación de DIR, pero el Directorio Activo incluye también un certificado asociado con una tarjeta inteligente registrada para el principal 110, el sistema 164 de generación de DIR podría incluir cualquiera o ambos tipos de autenticación como parte de la DIR devuelta al principal 110. Además, si se posibilita la capacidad de inicio de sesión único entre la máquina 111 principal y el sistema 164 de generación de DIR, el tipo de autenticación que se incluye en la DIR puede ser el tipo de autenticación usada por el principal 110 para autenticar a la máquina 111 principal.

Una vez que la o las DIR se ha/han generado mediante el sistema 164 de generación de DIR, se envían 390 al principal 110 mediante cualquiera de una diversidad de procedimientos, incluyendo correo electrónico, HTTP, etc. En algunas realizaciones, el fichero que incluye el o las DIR puede estar protegido por pin. Esto es debido a que, particularmente en el caso donde se envían múltiples DIR al principal 110, el fichero que contiene las DIR puede incluir material de clave criptográfica que debería protegerse frente a acceso no autorizado. El pin permite el establecimiento de un secreto compartido entre la máquina 111 principal y el sistema 164 de generación de DIR. Un fichero que contiene la o las DIR podría desencriptarse a continuación mediante el principal cuando se instalan las DIR en la máquina 111 principal. Se analizan adicionalmente a continuación procedimientos ejemplares para iniciar, aprobar y enviar las DIR.

Haciendo referencia ahora a la Figura 4, se ilustra un procedimiento 400. En la etapa 410 se recibe una solicitud para crear una DIR a través de un primer canal. Por ejemplo, el principal 110 puede usar un explorador de internet en la máquina 111 principal para solicitar una nueva DIR desde el sistema 164 de generación de DIR. En la etapa 420, se emite 420 una notificación a través de un segundo canal que la DIR ha solicitado. Por ejemplo, en respuesta a una solicitud para una nueva DIR desde el principal 110, el sistema 164 de generación de DIR o una aplicación que se ejecuta en la máquina 111 principal puede enviar una notificación de correo electrónico de que la solicitud se ha realizado. Esto puede actuar como una "comprobación" para asegurar que el principal 110 es el que solicita la DIR y no un impostor. En algunas realizaciones, el correo electrónico puede dirigirse a una dirección de correo electrónico conocida por el principal. En otras realizaciones, la notificación puede dirigirse a una tercera parte cuya política del administrador requiere aprobar la emisión de una nueva DIR para el principal 110 particular. Por ejemplo, algunas DIR pueden estar disponibles para ciertos empleados en una organización únicamente si sus directores aprueban la emisión. Este tipo de DIR puede usarse, por ejemplo, para obtener acceso a un grupo de trabajo confidencial.

Como se usa en el presente documento, un "canal" se refiere a la manera en la que se comunica la información en la emisión. La distinción entre diferentes canales en el procedimiento 400 es una lógica. Dos distintos canales podrían emplear alguna o todas del mismo enlace de comunicación físico o electrónico o diferentes rutas a la vez. Por ejemplo, podría enviarse una notificación en la etapa 420 a través del mismo enlace de comunicación (por

ejemplo, internet) como la aprobación en la etapa 430, pero los canales pueden ser lógicamente diferentes (por ejemplo, uno podría ser un correo electrónico y el otro podría ser un mensaje de HTTP).

En la etapa 430, se recibe una aprobación para la DIR a crear. Por ejemplo, el receptor de la notificación en la etapa 420 desde el sistema 364 de generación de DIR puede responder y aprobar la emisión de la DIR solicitada. Esto puede conseguirse de una diversidad de maneras. Por ejemplo, la notificación en la etapa 420 podría comprender un correo electrónico con un enlace a un sitio de aprobación alojado mediante el sistema 364 de generación de DIR.

En la etapa 440, se crea la DIR solicitada. Si la aprobación se denegara por el receptor de la notificación en la etapa 420, pueden tener lugar otros eventos. Por ejemplo, puede notificarse al administrador de que se realizó una solicitud no autorizada para una DIR.

Haciendo referencia ahora a la Figura 5, se muestra otro procedimiento ejemplar 500. En la etapa 510, se emite una notificación de que una DIR está disponible para un principal. Por ejemplo, el sistema 364 de generación de DIR podría enviar al principal 110 un correo electrónico que alerta al principal 110 de que una nueva DIR está disponible. Como alternativa, la notificación podría ir a una tercera parte, tal como el director del principal. Este tipo de notificación podría ser útil en una situación donde el administrador tiene, por ejemplo, el almacenamiento 168 de datos de identidad cambiado para incluir un descriptor adicional. El sistema 364 de generación de DIR podría a continuación usarse para notificar a todos los principales en una clase que califica al descriptor de que la nueva DIR está disponible. Por ejemplo, un director en una unidad de negocio particular puede solicitar a un administrador crear un nuevo descriptor para una DIR para usarse en conjunto con un objeto particular. Una vez que el administrador crea el descriptor, la notificación de todos los principales que el director desea tener la nueva DIR podría ser automática.

La notificación 510 podría incluirse también como parte de un flujo de trabajo de negocio general. Por ejemplo, cuando un nuevo principal empieza a trabajar en una organización, el departamento de recursos humanos podría capturar información acerca del principal a través del sistema 162 de captura de datos. Esos datos capturados podrían poner en marcha una serie de etapas automatizadas, incluyendo almacenar los datos de identidad relevantes con respecto al principal en el almacenamiento 168 de datos de identidad y notificar al principal 110 que una DIR está ahora disponible para él/ella. La notificación puede tomar muchas formas, incluyendo un correo electrónico al principal que incluye un enlace a un sitio web que comprende el sistema 164 de generación de DIR. Como alternativa, podría ejecutarse una aplicación en la máquina 111 principal que está adaptada para recibir un mensaje desde el sistema 164 de generación de DIR de que una nueva DIR está disponible para el principal 110 (por ejemplo, la aplicación podría generar un mensaje de ventana emergente, podría aparecer un icono en una barra de herramientas en la máquina 111 principal, etc.).

En la etapa 520, se recibe una solicitud para crear la DIR. Esta etapa puede conseguirse de nuevo de una diversidad de maneras. Por ejemplo, el principal 110 podría responder a un correo electrónico de notificación haciendo clic en un enlace que le lleva a una página web que proporciona al principal la opción de solicitar la DIR. Como alternativa, cuando una aplicación en la máquina 111 principal alerta al principal 110 de que la DIR está disponible, el principal podría solicitar la DIR en tal aplicación y la aplicación podría enviar un mensaje de vuelta al sistema 364 de generación de DIR para realizar la solicitud.

En la etapa 530, se crea la DIR según se solicita. La creación de la DIR puede conseguirse como se describe en cualquier otra parte en el presente documento. La DIR se envía a continuación 540 al principal, también como se describe en cualquier otra parte en el presente documento.

Haciendo referencia ahora a la Figura 6, se muestra otro procedimiento ejemplar 600. En la etapa 610, se interroga un sistema de generación de DIR para nuevas DIR que estén disponibles para el principal. Por ejemplo, la máquina 111 principal puede programarse para interrogar periódicamente el sistema 164 de generación de DIR a intervalos predeterminados. En la etapa 620, se determina si está disponible alguna nueva DIR para el principal. El sistema 164 de generación de DIR, por ejemplo, podría comprobar en el almacenamiento 168 de datos de identidad si se ha hecho disponible algún descriptor nuevo para el principal 110 desde el tiempo que se interrogó por última vez mediante la máquina 111 principal. En la etapa 630, se realiza una solicitud de que se cree la nueva DIR. Continuando el ejemplo, tras la recepción de la notificación de que una nueva DIR está disponible, el principal 110 podría solicitar que el sistema 164 de generación de DIR cree la nueva DIR. En la etapa 640, se recibe la nueva DIR (por ejemplo, podría recibirse una nueva DIR mediante la máquina 111 principal desde el sistema 164 de generación de DIR). Este procedimiento 600 es otro ejemplo de cómo podría simplificarse un trabajo de un administrador. Si todas las máquinas de los principales se programaran para interrogar nuevas DIR, por ejemplo, cuando un administrador crea un nuevo descriptor de DIR en el almacenamiento 168 de datos de identidad, la emisión y la entrega de las nuevas DIR es automática y no requiere trabajo adicional por cuenta del administrador.

Puede ser beneficioso también poder crear las DIR dinámicamente en respuesta a una política de seguridad de una parte confiante. Haciendo referencia ahora a la Figura 7, se ilustra un procedimiento de ejemplo 700. En la etapa 710, se solicita el acceso a una parte confiante. Por ejemplo, si la parte 120 confiante es un sitio web restringido, la máquina 111 principal intenta acceder al sitio web a través de un explorador. En la etapa 720, se deniega el acceso a la parte confiante y se recibe una política de seguridad desde la parte confiante. Continuando el ejemplo, la parte

120 confiante envía a la máquina 111 principal su política de seguridad y un mensaje de HTTP que redirige al explorador de la máquina 111 principal a una página web de autenticación. Una DIR que satisface la política de seguridad se solicita a continuación 730 desde un sistema de generación de DIR. En el ejemplo anterior, la máquina 111 principal puede comprobar en primer lugar si tiene una DIR suficiente y, si no, la máquina 111 principal puede programarse para consultar una caché local para el proveedor de identidad que ofrece las DIR que cumplen la política de seguridad de la parte 120 confiante. La máquina principal puede consultar también una lista pública de proveedores de DIR alojados mediante una tercera parte. El principal 110 puede a continuación elegir un proveedor de DIR y sistema de generación de DIR apropiados, tal como el sistema 164 de generación de DIR. En la etapa 740, se recibe la DIR. En el ejemplo anterior, la máquina 111 principal recibe la nueva DIR, que puede a continuación reenviarse al proveedor 115 de identidad para obtener el testigo de identidad necesario para obtener acceso a la parte 120 confiante.

En algunas realizaciones, la máquina 111 principal puede renviar la política de seguridad de la parte 120 confiante al sistema 164 de generación de DIR. El sistema 164 de generación de DIR puede a continuación comprobar el almacenamiento 168 de datos de identidad para determinar si las reclamaciones y otros requisitos expuestos en la política de seguridad pueden satisfacerse. Si es así, se crearía una DIR que cumple la política de seguridad. De esta manera, un principal puede obtener una DIR en una base según sea necesario, independientemente de si el administrador tiene un descriptor de identidad preconfigurado que cumple las necesidades de esa política de seguridad de la parte confiante particular.

Haciendo referencia ahora a la Figura 8, se muestra otro procedimiento ejemplar 800. En la etapa 810 se establece una política para un grupo de principales, que autoriza al grupo de principales de que está disponible una DIR. Con referencia al sistema 100 ejemplar de la Figura 1, un administrador podría usar el sistema de administrador para establecer una política en el almacenamiento 168 de datos de identidad que autoriza a todos los principales que son parte de un grupo particular a recibir una DIR particular. En algunas realizaciones, esto puede conseguirse por un administrador usando la característica de "Política de Grupo" disponible en el Directorio 169 Activo u otros medios para lanzar una aplicación del lado del cliente residente en la máquina 111 principal. En la etapa 820, se notifica al grupo de principales a los que la DIR está disponible. En el ejemplo anterior, se activa la aplicación del lado del cliente residente en la máquina 111 principal. Esto puede dar como resultado que se avise al principal 110 de que una nueva DIR está ahora disponible (por ejemplo, a través de una ventana emergente, un icono de barra de herramientas, etc.). La aplicación del lado del cliente puede tener su propio conjunto de reglas (por ejemplo, capacidad para que el principal 110 elija que se recuerde más tarde, para proporcionar al principal 110 únicamente una cierta cantidad de tiempo para recuperar la nueva DIR, etc.). En la etapa 830, se recibe una solicitud desde al menos un primer principal en el grupo de principales para crear la DIR. En algunas realizaciones esto puede implicar que el usuario autorice la creación de la DIR a través de la aplicación del lado del cliente residente en la máquina 111 principal. En otras realizaciones, la aplicación del lado del cliente puede solicitar la DIR sin implicación adicional del principal 110. En la etapa 840, se crea la DIR para el primer principal.

La Figura 9 ilustra un dispositivo 900 informático general (también denominado en el presente documento como un ordenador o sistema informático), que puede usarse para implementar las realizaciones descritas en el presente documento. El dispositivo 900 informático es únicamente un ejemplo de un entorno informático y no se pretende para sugerir ninguna limitación en cuanto al alcance de uso o funcionalidad de las arquitecturas informáticas y de red. Ni debería interpretarse que el dispositivo 900 informático tiene alguna dependencia o requisito relacionado con uno cualquiera o combinación de los componentes ilustrados en el dispositivo 900 informático de ejemplo. En las realizaciones, el dispositivo 900 informático puede usarse, por ejemplo, como una máquina 111 principal, sistema 164 de generación de DIR, sistema 162 de captura de datos, IIS 166, almacenamiento 168 de datos de identidad, directorio 169 activo, sistema 160 de administrador, proveedor 115 de identidad, o parte 120 confiante como se ha descrito anteriormente con respecto a la Figura 1.

En su configuración más básica, el dispositivo 900 informático incluye típicamente al menos una unidad 902 de procesamiento y memoria 904. Dependiendo de la configuración exacta y tipo de dispositivo informático, la memoria 904 puede ser volátil (tal como RAM), no volátil (tal como ROM, memoria flash, etc.) o alguna combinación de las dos. Esta configuración más básica se ilustra en la Figura 9 mediante la línea 906 discontinua. La memoria 904 de sistema almacena aplicaciones que se ejecutan en el dispositivo 900 informático. Además de las aplicaciones, la memoria 904 puede almacenar también información que se usa en operaciones que se realizan mediante el dispositivo 900 informático, tal como una solicitud 910 de creación de DIR y/o una notificación 911 de disponibilidad de DIR, como se ha descrito anteriormente con respecto a las Figuras 1-8.

Adicionalmente, el dispositivo 900 informático puede tener también características/funcionalidad adicionales. Por ejemplo, el dispositivo 900 informático puede incluir también almacenamiento 908 adicional (extraíble y/o no extraíble) incluyendo, pero sin limitación, discos o cinta magnéticos u ópticos. Tal almacenamiento adicional se ilustra en la Figura 9 mediante el almacenamiento 908. El medio de almacenamiento informático incluye memoria volátil y no volátil, extraíble y no extraíble implementada en cualquier procedimiento o tecnología para almacenamiento de información tal como instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos. La memoria 904 y el almacenamiento 908 son ejemplos de medio de almacenamiento informático. El medio de almacenamiento informático incluye, pero sin limitación, RAM, ROM, EEPROM, memoria flash u otra tecnología de memoria, CD-ROM, discos versátiles digitales (DVD) u otro almacenamiento óptico,

casetes magnéticas, cinta magnética, almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para almacenar la información deseada y que pueda accederse mediante el dispositivo 900 informático. Cualquier medio de almacenamiento informático de este tipo puede ser parte del dispositivo 900 informático.

Como apreciarán los expertos en la materia, el almacenamiento 908 puede almacenar una diversidad de información. Entre otros tipos de información, el almacenamiento 908 puede almacenar una representación 930 de identidad digital (por ejemplo, en el caso de una máquina principal) o un testigo 945 de identidad (por ejemplo, en el caso de un proveedor de identidad).

El dispositivo 900 informático puede contener también conexión o conexiones 912 de comunicaciones que permiten al sistema comunicar con otros dispositivos. La conexión o conexiones 912 de comunicaciones son un ejemplo de medio de comunicación. El medio de comunicación típicamente incorpora instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos en una señal de datos modulada tal como una onda portadora u otro mecanismo de transporte e incluye cualquier medio de entrega de información. La expresión "señal de datos modulada" significa una señal que tiene una o más de sus características establecidas o cambiadas de tal manera para codificar información en la señal. A modo de ejemplo, y no como limitación, el medio de comunicación incluye medio cableado tal como una red cableada o conexión cableada directa, y medio inalámbrico tal como acústico, RF, infrarrojos y otros medios inalámbricos. La expresión medio legible por ordenador como se usa en el presente documento incluye tanto medio de almacenamiento como medio de comunicación.

El dispositivo 900 informático puede tener también el dispositivo o dispositivos 914 de entrada tales como el teclado, ratón, lápiz, dispositivo de entrada de voz, dispositivo de entrada táctil, etc. Pueden incluirse también dispositivo o dispositivos 916 de salida tales como una pantalla, altavoces, impresora, etc. Todos estos dispositivos son bien conocidos en la técnica y no necesitan analizarse en profundidad en este punto.

Las diversas realizaciones anteriormente descritas se proporcionan a modo de ilustración únicamente y no deberían interpretarse como limitantes. Los expertos en la materia reconocerán fácilmente que pueden realizarse diversas modificaciones y cambios a las realizaciones anteriormente descritas sin alejarse del alcance de la divulgación o de las siguientes reivindicaciones.

Lo siguiente es una lista de realizaciones preferidas adicionales de la invención:

Realización 1: un sistema (100) para aprovisionar una representación (930) de identidad digital para un principal (110), que comprende:

un sistema (164) de generación de representación de identidad digital para generar la representación (930) de identidad digital;

un proveedor (115) de identidad para generar un testigo (150) de identidad en respuesta a recibir una solicitud de testigo de identidad, en el que la solicitud de testigo de identidad se genera en respuesta a la selección de la representación (930) de identidad digital; y

un almacenamiento (168) de datos de identidad, conectado de manera operativa al proveedor (115) de identidad y al sistema (164) de generación de representación de identidad digital;

en el que el sistema (164) de generación de representación de identidad digital accede al almacenamiento (168) de datos de identidad al generar la representación (930) de identidad digital y el proveedor (115) de identidad accede al almacenamiento (168) de datos de identidad al generar el testigo (150) de identidad.

Realización 2: el sistema de la realización 1, en el que el sistema de generación de representación de identidad digital está adaptado adicionalmente para:

recibir una solicitud a través de un primer canal para crear la representación de identidad digital para el principal;

emitir una notificación a través de un segundo canal de que se ha solicitado la representación de identidad digital; y

recibir una aprobación para que se cree la representación de identidad digital.

Realización 3: el sistema de la realización 1, en el que el sistema de generación de representación de identidad digital está adaptado adicionalmente para:

emitir una notificación de que una o más representaciones de identidad digital están disponibles para el principal; y

recibir una solicitud para crear la una o más representaciones de identidad digital.

Realización 4: el sistema de la realización 1, que comprende además una máquina principal, en el que la máquina principal está adaptada para:

interrogar el sistema de generación de representación de identidad digital para determinar si está disponible una nueva representación de identidad digital para el principal;

solicitar que se cree la nueva representación de identidad digital; y

recibir la nueva representación de identidad digital.

Realización 5: el sistema de la realización 1, que comprende además una máquina de administrador, controlada por un administrador y adaptada para establecer una política de que se permite a un grupo de principales acceder a la representación de identidad digital, y en el que se notifica al grupo de principales de que la representación de identidad digital está disponible y el sistema de generación de representación de identidad digital está adaptado para recibir una solicitud desde al menos un primer principal en el grupo de principales para crear la representación de identidad digital.

Realización 6: el sistema de la realización 1, en el que el almacenamiento de datos de identidad incluye al menos una primera categoría de datos y una segunda categoría de datos, que comprende además:

una máquina de administrador, conectada de manera operativa al almacenamiento de datos de identidad, para crear un cambio en al menos la primera categoría de datos;

en el que, después del cambio, el sistema de generación de representación de identidad digital genera las representaciones de identidad digital que reflejan el cambio y el proveedor de identidad genera testigos de identidad que reflejan el cambio.

Realización 7: el sistema de la realización 6, en el que, si el cambio afecta a la validez de cualquier representación de identidad digital ya generada por el sistema de generación de representación de identidad digital, el sistema de generación de representación de identidad digital notifica a cada principal que recibió la representación de identidad digital afectada y crea una nueva representación de identidad digital que refleja el cambio.

Realización 8: el sistema de la realización 1, en el que el sistema de generación de representación de identidad digital está adaptado adicionalmente para proteger criptográficamente la representación de identidad digital y enviar la representación de identidad digital criptográficamente protegida a una máquina principal.

Realización 9: el sistema de la realización 1, que comprende además:

una máquina de administrador para crear un primer descriptor de representación de identidad digital; y

una máquina principal para solicitar una representación de identidad digital conforme al primer descriptor de representación de identidad digital.

Realización 10: un procedimiento (300) para aprovisionar una representación de identidad digital para un principal, que comprende:

autenticar (330) el principal a un sistema (164) de generación de representación de identidad digital usando información de inicio de sesión;

recibir (370) una solicitud para una representación (930) de identidad digital;

generar (380) la representación (930) de identidad digital para el principal (110), en el que la representación (930) de identidad digital incluye al menos alguna de la información de inicio de sesión.

Realización 11: el procedimiento de la realización 10, en el que la información de inicio de sesión comprende al menos alguna información de inicio de sesión usada para iniciar sesión en una máquina principal.

Realización 12: el procedimiento de la realización 10, que comprende además la etapa de:

crear un primer descriptor de representación de identidad digital;

en el que la representación de identidad digital solicitada se ajusta al primer descriptor de representación de identidad digital.

Realización 13: el procedimiento de la realización 10, que comprende además la etapa, antes de la etapa de autenticación, de:

emitir una notificación al principal de que la representación de identidad digital está disponible para el principal.

Realización 14: el procedimiento de la realización 10, en el que la etapa de recibir una solicitud comprende recibir la solicitud para la representación de identidad digital a través de un primer canal, y que comprende además las etapas de:

emitir una notificación a través de un segundo canal de que la representación de identidad digital se ha solicitado; y

recibir la aprobación para que se genere la representación de la identidad digital.

Realización 15: el procedimiento de la realización 10, que comprende además la etapa, antes de la etapa de generación, de:

determinar si el principal es un miembro de un grupo aprobado para recibir la representación de identidad digital.

Realización 16: el procedimiento de la realización 10, que comprende además la etapa de:

responder a una solicitud en cuanto a si alguna representación de identidad digital está disponible para el principal.

Realización 17: un procedimiento (300) para aprovisionar una representación (930) de identidad digital para un principal (110), que comprende las etapas de:

generar (350) un primer descriptor de representación de identidad digital y un segundo descriptor de representación de identidad digital;

enviar (360) el primer y segundo descriptores de representación de identidad digital al principal (110);

recibir (370) una solicitud desde el principal (110) para al menos una primera representación (930) de identidad digital conforme al primer descriptor de representación de identidad digital;

crear al menos la primera representación (930) de identidad digital.

Realización 18: el procedimiento de la realización 17, en el que la solicitud se recibe a través de un primer canal, y que comprende además las etapas de:

emitir una notificación a través de un segundo canal de que la primera representación de identidad digital se ha solicitado; y

recibir la aprobación para que se genere la primera representación de identidad digital.

Realización 19: un procedimiento (700) para aprovisionar una representación (930) de identidad digital para un principal (110), que comprende las etapas de:

solicitar (710) acceso a una parte (120) confiante;

recibir (720) desde la parte (120) confiante una denegación de acceso;

solicitar (730) desde un sistema (164) de generación de representación de identidad digital una representación (930) de identidad digital que es suficiente para obtener el acceso para la parte (120) confiante;

recibir (740) la representación (930) de identidad digital.

Realización 20: el procedimiento de la realización 19, en el que la etapa de recibir desde la parte confiante una denegación de acceso incluye recibir una política de seguridad desde la parte confiante y que comprende además la etapa de:

enviar la representación de identidad digital a un proveedor de identidad; y

obtener un testigo de identidad suficiente para satisfacer la política de seguridad de la parte confiante.

REIVINDICACIONES

1. Un sistema (100) para aprovisionar una representación (930) de identidad digital para un principal (110), que comprende:

un sistema (164) de generación de representación de identidad digital adaptado para generar una representación de identidad digital, DIR (930) para un principal (110), y para enviar la DIR al principal, siendo la DIR específica para un proveedor (115) de identidad y que incluye una política de emisión del proveedor de identidad para testigos (150, 945) de identidad, así como reclamaciones acerca del principal;
el proveedor (115) de identidad, adaptado para recibir la DIR, para generar un testigo (150) de identidad que corresponde a la DIR y para enviar el testigo de identidad al principal, rellenándose el testigo de identidad con información acerca del principal que corresponde a las reclamaciones incluidas en la DIR para satisfacer una política de seguridad; y
un almacenamiento (168) de datos de identidad, conectado de manera operativa al proveedor de identidad y al sistema de generación de representación de identidad digital, adaptado para almacenar las reclamaciones acerca del principal incluidas en la DIR y la correspondiente información acerca del principal usada para rellenar el testigo de identidad,
en el que la generación de la DIR mediante el sistema de generación de representación de identidad digital y la generación del testigo de identidad mediante el proveedor de identidad se realizan accediendo al mismo almacenamiento de datos de identidad para asegurar que la información acerca del principal que corresponde a las reclamaciones contenidas en la DIR está de hecho disponible en el almacenamiento de datos de identidad para rellenar el testigo de identidad.

2. El sistema de la reivindicación 1, en el que el sistema de generación de representación de identidad digital está adaptado adicionalmente para realizar uno de:

recibir una solicitud a través de un primer canal para crear la DIR para el principal, emitir una notificación a través de un segundo canal de que la DIR ha sido solicitada, y recibir una aprobación para que se cree la DIR; y
emitir una notificación de que uno o más descriptores de representación de identidad digital están disponibles para el principal, y recibir una solicitud para crear una o más DIR que corresponden al uno o más descriptores de representación de identidad digital.

3. El sistema de la reivindicación 1, que comprende además una máquina (111) principal, en el que la máquina principal está adaptada para:

interrogar (610) el sistema de generación de representación de identidad digital para determinar si un nuevo descriptor de representación de identidad digital está disponible para el principal;
solicitar (630) que se cree una nueva DIR que corresponde al descriptor de representación de identidad digital disponible recientemente; y
recibir (640) la nueva DIR.

4. El sistema de la reivindicación 1, que comprende además una máquina (160) de administrador, controlada por un administrador y adaptada para establecer una política de que se permite a un grupo de principales acceder a la DIR, y en el que se notifica al grupo de principales de que la DIR está disponible y el sistema de generación de representación de identidad digital está adaptado para recibir una solicitud desde al menos un primer principal en el grupo de principales para crear la DIR.

5. El sistema de la reivindicación 1, que comprende además:

una máquina (160) de administrador, conectada de manera operativa al almacenamiento de datos de identidad y adaptada para crear un cambio que afecta una validez de DIR ya emitidas,
en el que, después del cambio, el sistema de generación de representación de identidad digital está adaptado adicionalmente para notificar a cada principal que recibió una DIR afectada por el cambio y para generar nuevas DIR que reflejan el cambio, y
en el que el proveedor de identidad está adaptado adicionalmente para generar testigos de identidad que reflejan el cambio.

6. El sistema de la reivindicación 1, en el que el sistema de generación de representación de identidad digital está adaptado adicionalmente para proteger criptográficamente la DIR y para enviar la DIR criptográficamente protegida a una máquina (111) principal.

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

una máquina (160) de administrador adaptada para crear un primer descriptor de representación de identidad digital; y
una máquina (111) principal adaptada para solicitar una DIR conforme al primer descriptor de representación de identidad digital.

8. Un procedimiento para aprovisionar una representación (930) de identidad digital para un principal (110), que comprende:

generar, en un sistema (164) de generación de representación de identidad digital, una representación de identidad digital, DIR (930) para un principal (110), siendo la DIR específica para un proveedor (115) de identidad y que incluye una política de emisión del proveedor de identidad para testigos de identidad, así como reclamaciones acerca del principal;
enviar, mediante el sistema de generación de representación de identidad digital, la DIR al principal (110);
recibir la DIR en el proveedor de identidad;
generar, mediante el proveedor de identidad, un testigo (150) de identidad que corresponde a la DIR, rellenándose el testigo de identidad con información acerca del principal que corresponde a las reclamaciones incluidas en la DIR para satisfacer una política de seguridad; y enviar, mediante el proveedor de identidad, el testigo de identidad al principal,
en el que las reclamaciones acerca del principal incluidas en la DIR y la correspondiente información acerca del principal usada para rellenar el testigo de identidad se almacenan en un mismo almacenamiento (168) de datos de identidad, y
en el que la generación de la DIR mediante el sistema de generación de representación de identidad digital y la generación del testigo de identidad mediante el proveedor de identidad se realizan accediendo al mismo almacenamiento de datos de identidad para asegurar que la información acerca del principal que corresponde a las reclamaciones contenidas en la DIR están de hecho disponibles en el almacenamiento de datos de identidad para rellenar el testigo de identidad.

9. El procedimiento de la reivindicación 8, en el que la etapa de generar la DIR comprende:

autenticar (330) el principal para el sistema (164) de generación de representación de identidad digital usando información de inicio de sesión;
recibir (370) una solicitud para la DIR; y
generar (380) la DIR para el principal, en el que la DIR incluye al menos alguna de la información de inicio de sesión.

10. El procedimiento de la reivindicación 9, en el que la información de inicio de sesión comprende al menos alguna información de inicio de sesión usada para iniciar sesión en una máquina principal.

11. El procedimiento de la reivindicación 9, que comprende además uno de:

crear un primer descriptor de representación de identidad digital, en el que la DIR solicitada se ajusta al primer descriptor de representación de identidad digital;
antes de la etapa de autenticación, emitir una notificación al principal de que la DIR está disponible para el principal;
antes de la etapa de generación, determinar si el principal es un miembro de un grupo aprobado para recibir la DIR; y
responder a una solicitud en cuanto a si alguna DIR está disponible para el principal.

12. El procedimiento de la reivindicación 9, en el que la etapa de recibir una solicitud comprende recibir la solicitud para la DIR a través de un primer canal, y que comprende además las etapas de:

emitir una notificación a través de un segundo canal de que la DIR se ha solicitado; y
recibir la aprobación para que se genere la DIR.

13. Un procedimiento (700) en una máquina (111) principal para aprovisionar una representación de identidad digital, DIR (930), para un principal (110), que comprende las etapas de:

solicitar (710) acceso a una parte (120) confiante;
recibir (720) desde la parte confiante una denegación de acceso;
solicitar (730) desde un sistema (164) de generación de representación de identidad digital una DIR que es suficiente para obtener el acceso para la parte (120) confiante, siendo la DIR específica para un proveedor (115) de identidad y que incluye una política de emisión del proveedor de identidad para testigos de identidad, así como reclamaciones acerca del principal;
recibir (740) la DIR;
enviar la DIR al proveedor de identidad; y
obtener un testigo de identidad que se rellena con información acerca del principal que corresponde a las reclamaciones incluidas en la DIR para satisfacer la política de seguridad de la parte confiante,
en el que las reclamaciones acerca del principal incluidas en la DIR y la correspondiente información acerca del principal usada para rellenar el testigo de identidad se obtienen a partir de un mismo almacenamiento (168) de datos de identidad para asegurar que la información acerca del principal que corresponde a las reclamaciones contenidas en la DIR está de hecho disponible en el almacenamiento de datos de identidad para rellenar el testigo de identidad.

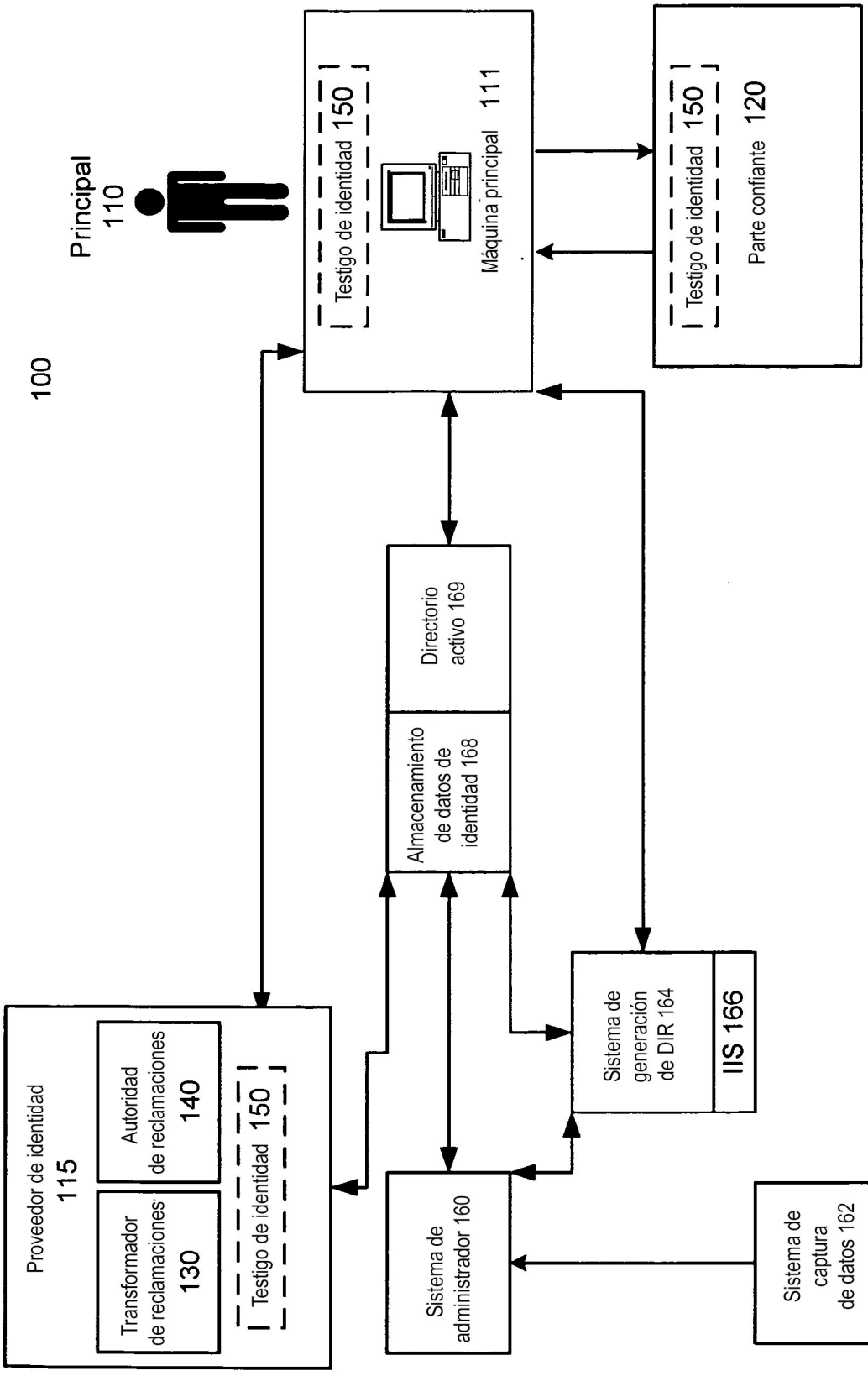
100
Principal
110
Testigo de identidad 150
Máquina principal 111
Testigo de identidad 150
Parte confiante 120
Directorio activo 169
Almacenamiento de datos de identidad 168
Proveedor de identidad 115
Autoridad de reclamaciones 140
Transformador de reclamaciones 130
Testigo de identidad 150
Sistema de generación de DIR 164
IIS 166
Sistema de administrador 160
Sistema de captura de datos 162

Fig. 1

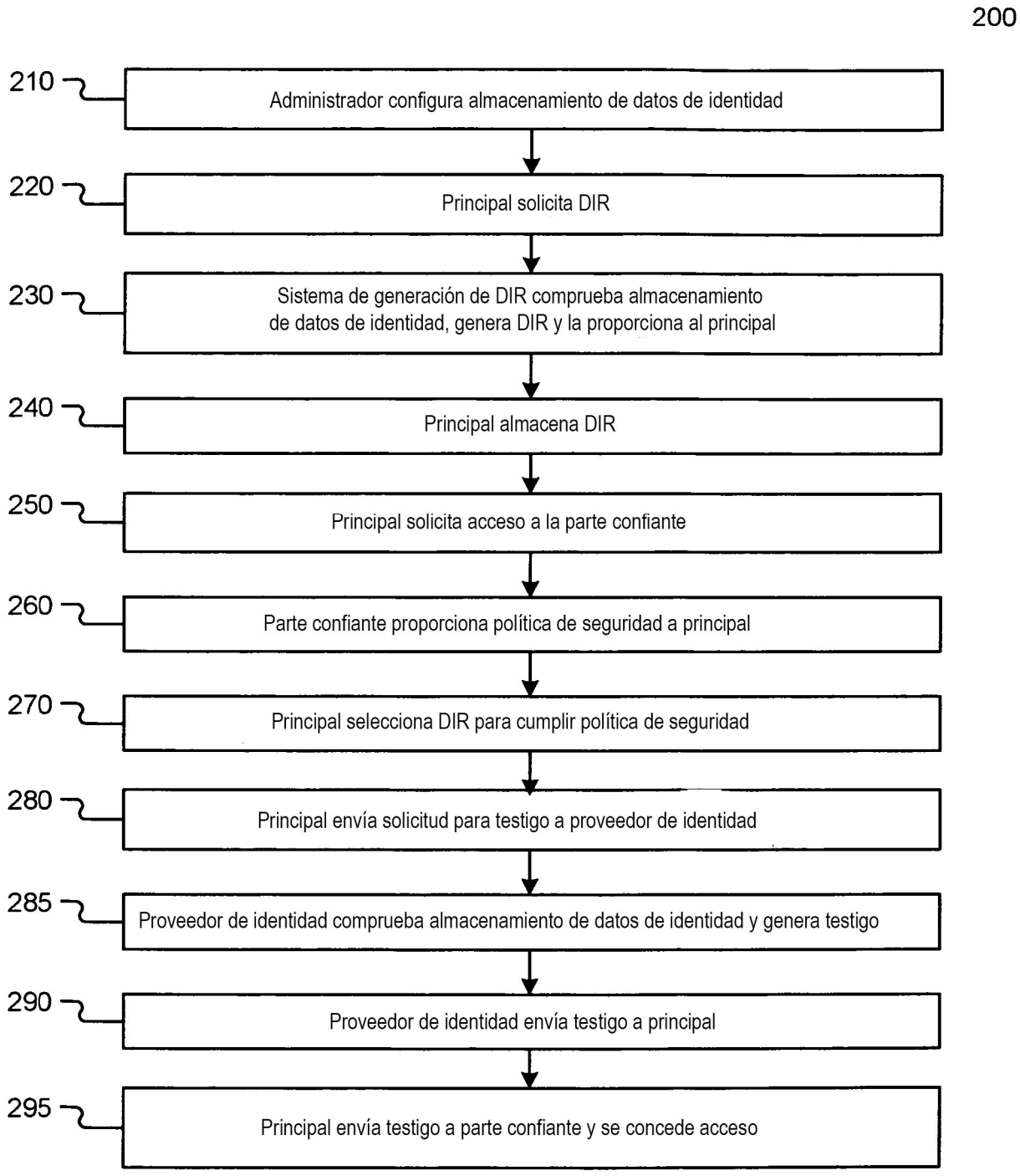
200
210
Administrador configura almacenamiento de datos de identidad
220
Principal solicita DIR
230
Sistema de generación de DIR comprueba almacenamiento de datos de identidad, genera DIR y la proporciona al principal
240
Principal almacena DIR
250
Principal solicita acceso a la parte confiante
260
Parte confiante proporciona política de seguridad a principal
270
Principal selecciona DIR para cumplir política de seguridad
280
Principal envía solicitud para testigo a proveedor de identidad
285
Proveedor de identidad comprueba almacenamiento de datos de identidad y genera testigo
290
Proveedor de identidad envía testigo a principal
295
Principal envía testigo a parte confiante y se concede acceso

Fig. 2

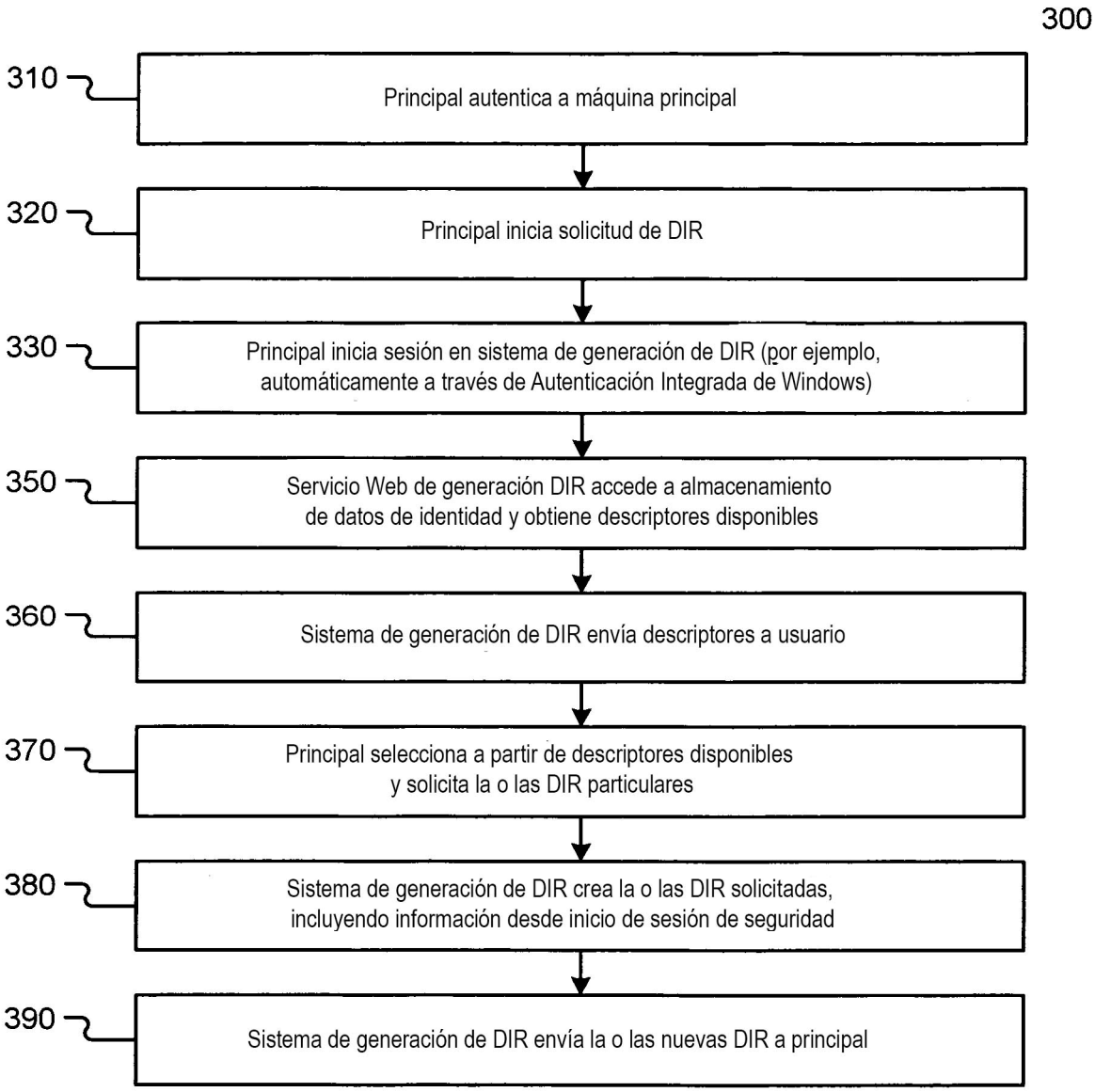
300
310
Principal autentica a máquina principal
320
Principal inicia solicitud de DIR
330
Principal inicia sesión en sistema de generación de DIR (por ejemplo, automáticamente a través de Autenticación Integrada de Windows)
350
Servicio Web de generación DIR accede a almacenamiento de datos de identidad y obtiene descriptores disponibles
360
Sistema de generación de DIR envía descriptores a usuario
370
Principal selecciona a partir de descriptores disponibles y solicita la o las DIR particulares
380
Sistema de generación de DIR crea la o las DIR solicitadas, incluyendo información desde inicio de sesión de seguridad
390
Sistema de generación de DIR envía la o las nuevas DIR a principal

Fig. 3

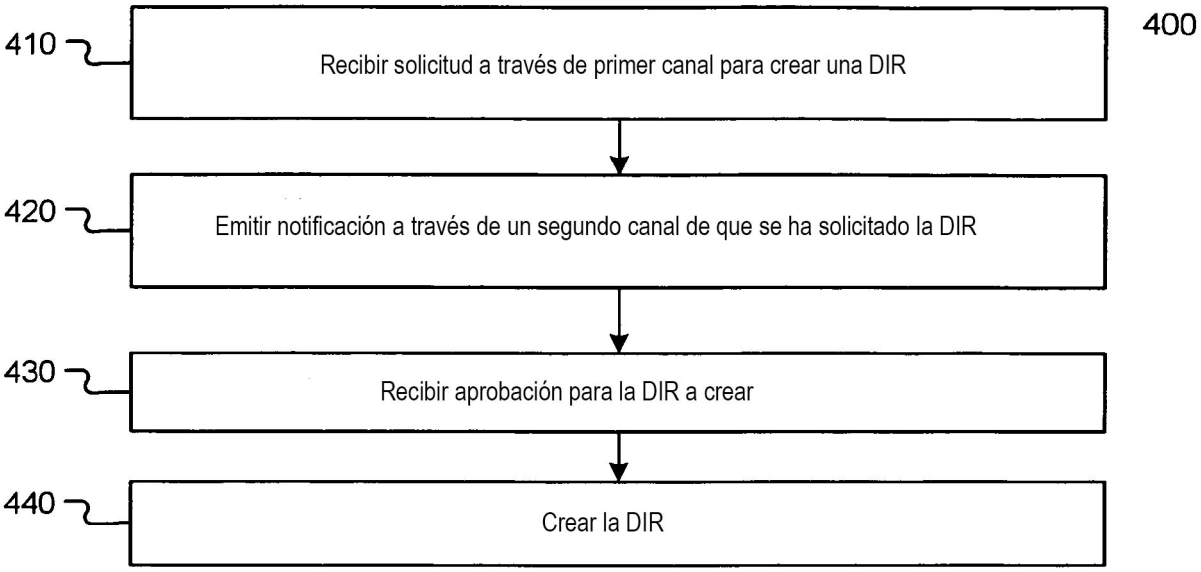
400
410
Recibir solicitud a través de primer canal para crear una DIR
420
Emitir notificación a través de un segundo canal de que se ha solicitado la DIR
430
Recibir aprobación para la DIR a crear
440
Crear la DIR

Fig. 4

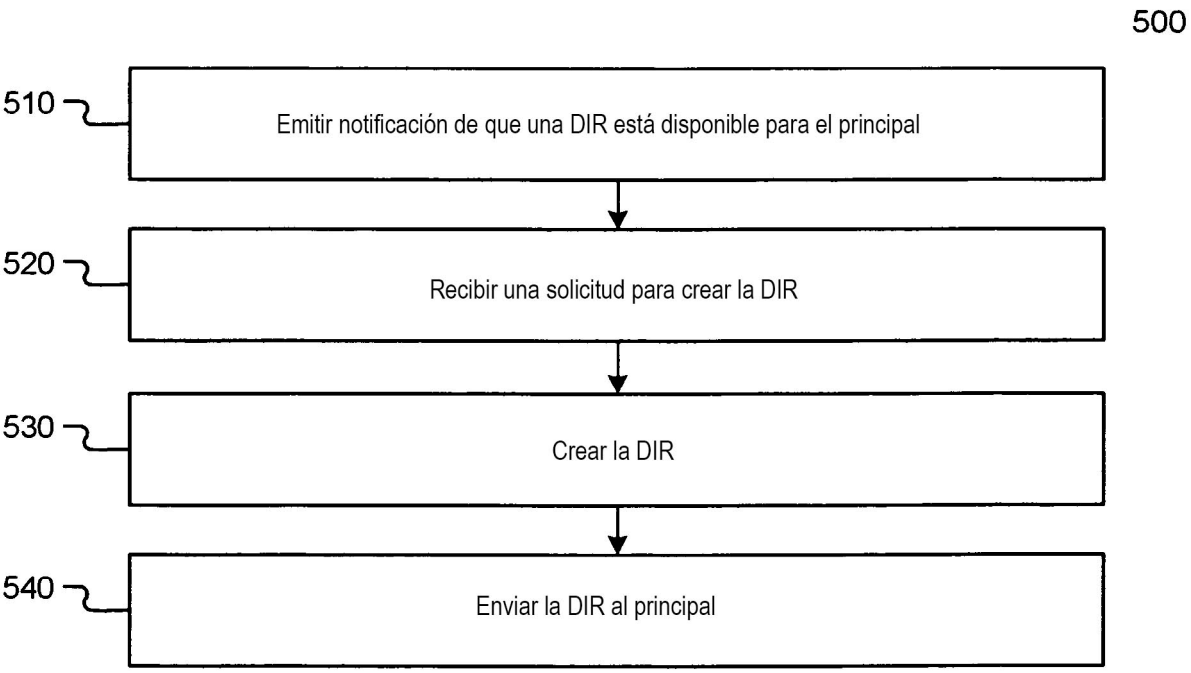
500
510
Emitir notificación de que una DIR está disponible para el principal
520
Recibir una solicitud para crear la DIR
530
Crear la DIR
540
Enviar la DIR al principal

Fig. 5

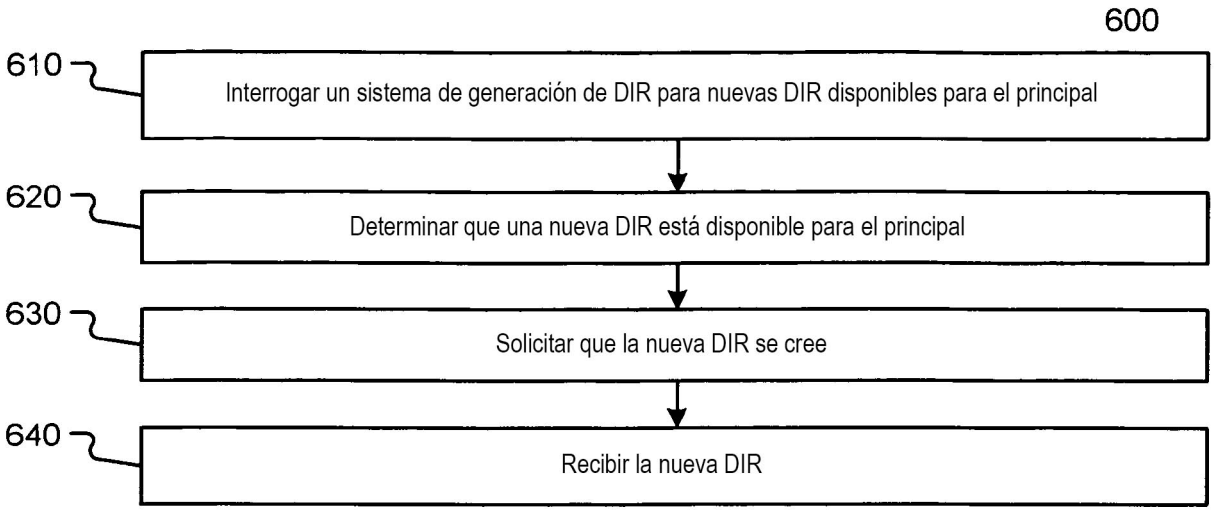
600
610
Interrogar un sistema de generación de DIR para nuevas DIR disponibles para el principal
620
Determinar que una nueva DIR está disponible para el principal
630
Solicitar que la nueva DIR se cree
640
Recibir la nueva DIR

Fig. 6

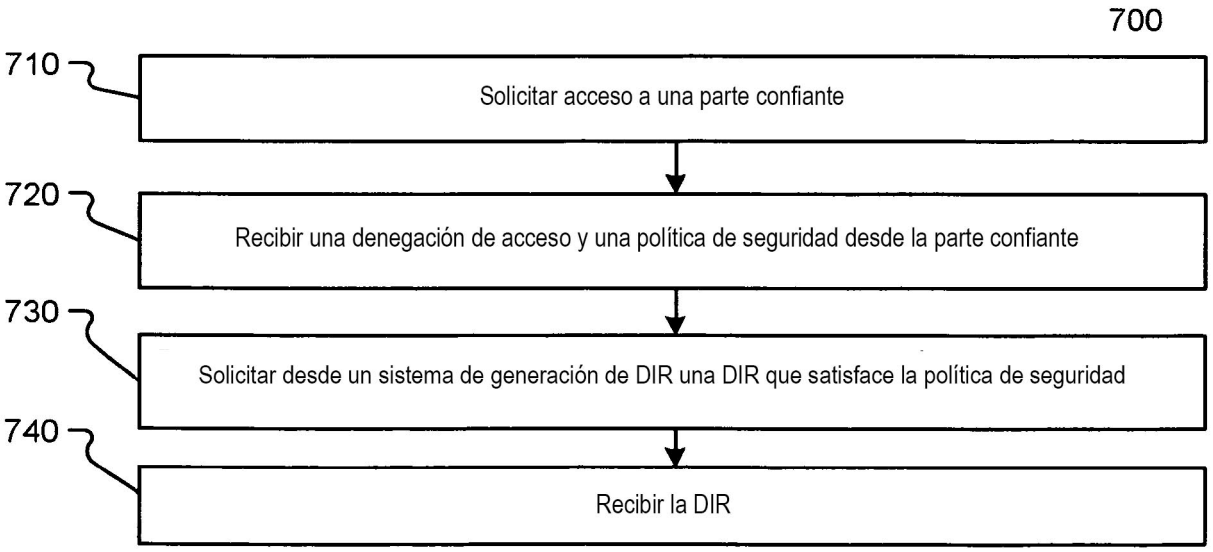
700
710
Solicitar acceso a una parte confiante
720
Recibir una denegación de acceso y una política de seguridad desde la parte confiante
730
Solicitar desde un sistema de generación de DIR una DIR que satisface la política de seguridad
740
Recibir la DIR

Fig. 7

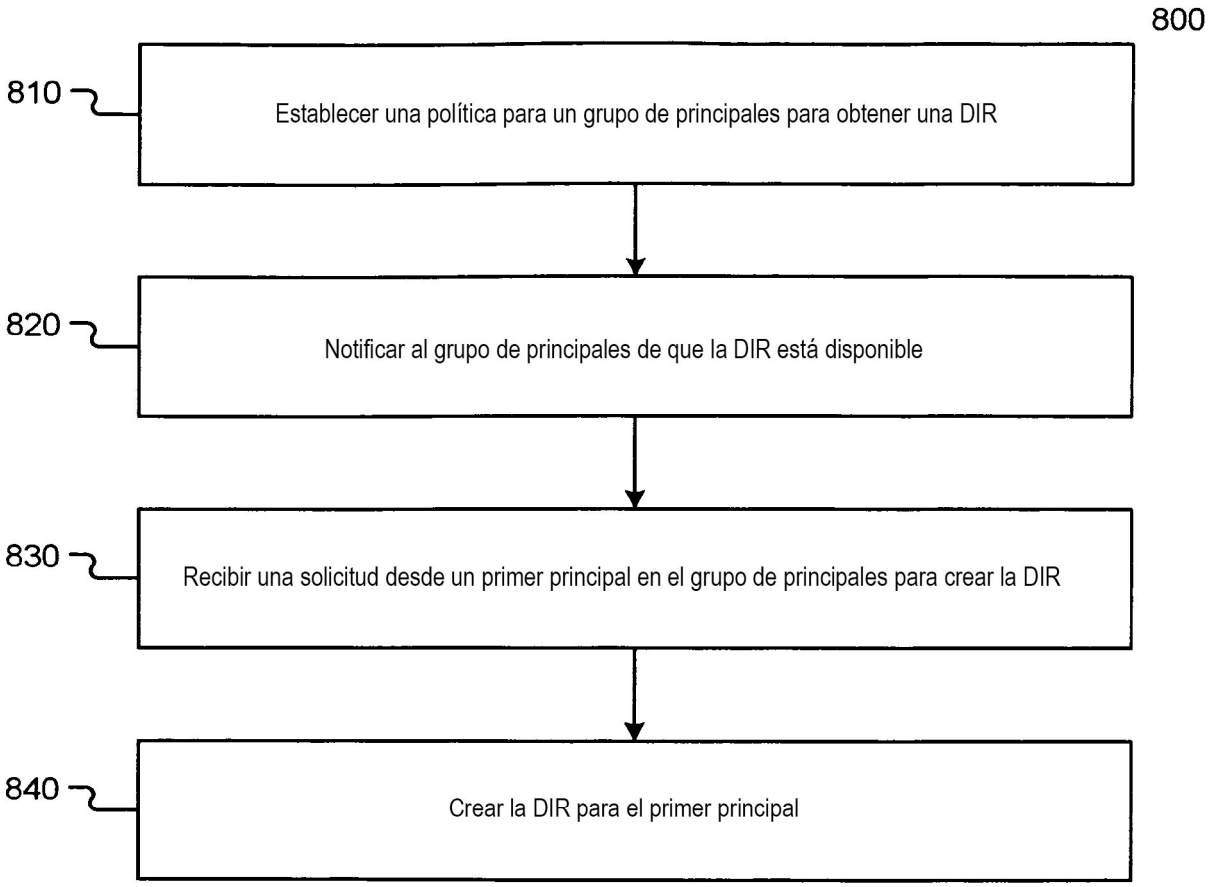
800
810
Establecer una política para un grupo de principales para obtener una DIR
820
Notificar al grupo de principales de que la DIR está disponible
830
Recibir una solicitud desde un primer principal en el grupo de principales para crear la DIR
840
Crear la DIR para el primer principal

Fig. 8

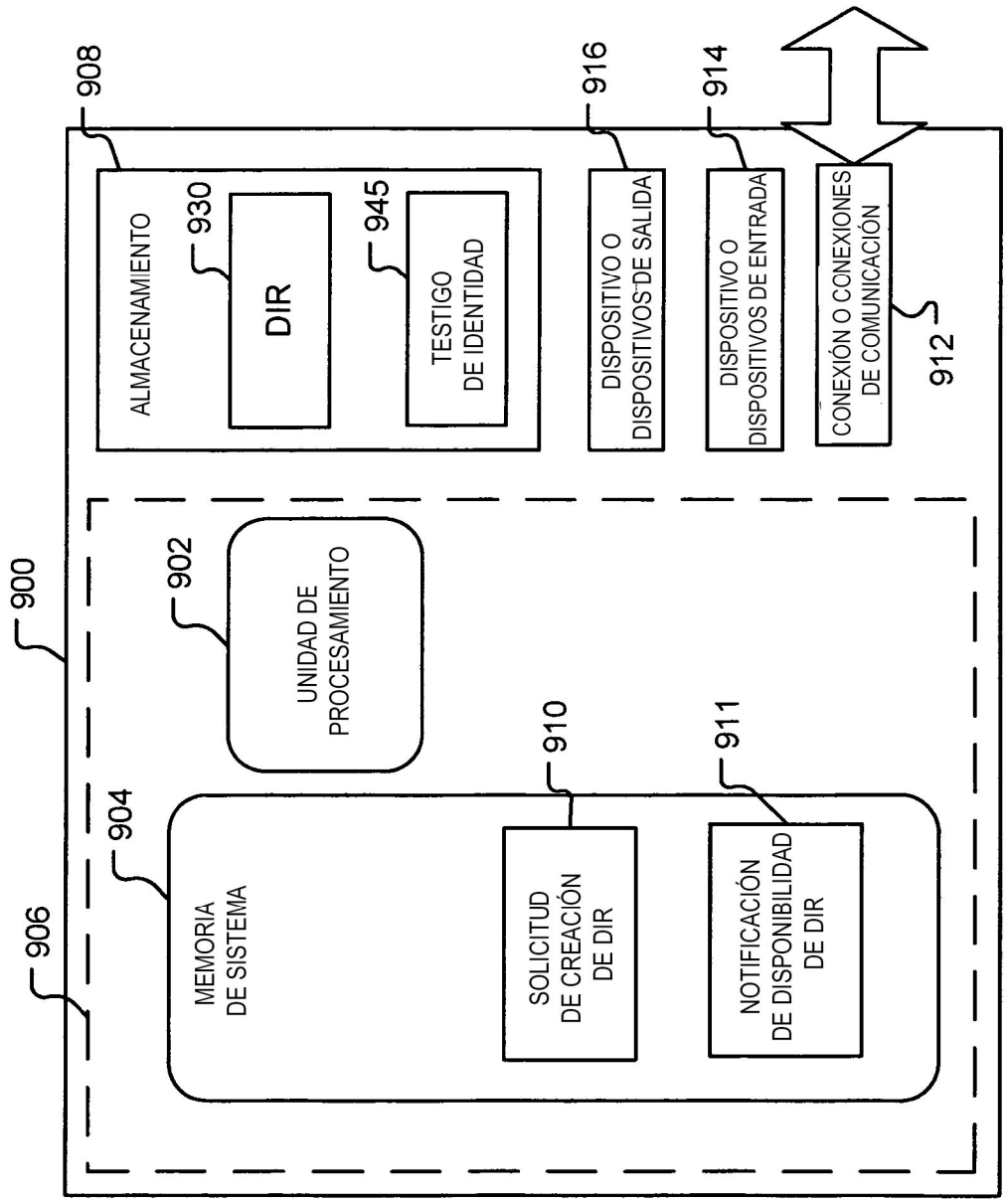
900
902
UNIDAD DE PROCESAMIENTO
904
MEMORIA DE SISTEMA
906
908
ALMACENAMIENTO
930
DIR
945
TESTIGO DE IDENTIDAD
910
SOLICITUD DE CREACIÓN DE DIR
911
NOTIFICACIÓN DE DISPONIBILIDAD DE DIR
916
DISPOSITIVO O DISPOSITIVOS DE SALIDA
914
DISPOSITIVO O DISPOSITIVOS DE ENTRADA
912
CONEXIÓN O CONEXIONES DE COMUNICACIÓN

Fig. 9