Arquitectura de Referencia IAM (v2)

Por George B. Dobbs

Por comentarios sobre este artículo, contacte nuestro Repositorio GitHub o reporte un problema

Tabla de contenido

Resumen

Este artículo aproxima un modelo de referencia para la organización de la presentación de los detalles técnicos asociados con las muchas implementaciones posibles de los conceptos de la arquitectura de la administración de identidades y accesos (IAM, por sus siglas en inglés). Tanto el modelo como el conjunto de componentes abstractos que provee son conceptuales.

En el Cuerpo de Conocimiento de IDPro encontrará artículos adicionales que ofrecen casos de uso con contenido técnico específico basado en los conceptos abstractos de este documento.

Introducción

Se dice que todos los modelos están equivocados y sin embargo algunos son útiles.[1] Este modelo busca encontrar cierto nivel de generalización que sea ampliamente útil. Cuando generaliza demasiado, el modelo queda desconectado de la realidad volviéndose inútil. Cuando se vuelve demasiado específico, el modelo solo sirve para algunos casos.

Esta Arquitectura de Referencia de la IAM se inclina más hacia la implementación técnica y aborda algunas facetas legales, procesos y capacidades. La amplitud de este abordaje apunta a proveer al lector un conjunto de conceptos que puedan ser aplicados a la hora de pensar en la IAM.

El principio sobre el cual se basa este modelo supone que la administración de identidades y accesos puede separarse de su uso (en la mayoría de los casos esto es así). Este concepto puede aplicarse tanto a sistemas distribuidos como a sistemas autónomos. Así que cuando veas a la IAM trabajando conjuntamente en una aplicación, esto significa probablemente que se trata de dos sistemas físicos independientes. En su defecto, puede significar que se trata de partes independientes de un software que está ejecutándose en un mismo sistema.

Al ofrecer un conjunto común de términos y conceptos que pueden ser utilizados en todas las arquitecturas IAM, este artículo busca habilitar el debate sobre casos de uso más específicos. Si bien el modelo incorpora la guía de varios documentos de estándares y buenas prácticas, la estructura primordial del modelo tuvo como base el marco ISO/IEC.[2]

---

[1] Colaboradores de Wikipedia, "All models are wrong," *Wikipedia, La Enciclopedia Libre,* https://en.wikipedia.org/w/index.php?title=All_models_are_wrong&oldid=1111346950 (consultado el 28 de noviembre de 2022).

[2] ISO/IEC 24760-1 Segunda edición “Seguridad y Privacidad TI — Un marco para la gestión de identidades — Parte 1: Terminología y conceptos,” https://www.iso.org/standard/77582.html y ISO/IEC 24760-2, 2015 “Tecnología de la Información — Técnicas de Seguridad — Un marco para la

En el ánimo de simplificar y facilitar la comprensión, el Lenguaje Unificado de Modelado (UML, por sus siglas en inglés) se eliminó del alcance de este documento mientras que el modelo IAM se extendió para poder abarcar los aspectos de autorización, gobernanza y gestión de riesgos.

Algunos de los nombres ISO/IEC fueron cambiados por términos de uso común. En algunos casos los nombres ISO se utilizan de manera más abarcativa que en su definición original.

Con el fin de adoptar la terminología más útil, el modelo ha sido cotejado con las definiciones FICAM,[3] Internet2,[4] y NIST SP-800-63,[5] así como con las infraestructuras NIST Zero Trust,[6] y con el *Identity Stack* presentado en *Identiverse 2019*.[7]

El modelo es compatible con varios niveles de complejidad de sistema. Por ejemplo, puede usarse:

- en un entorno de Sistema Distribuido, donde la arquitectura puede tener un Tercero Confiable (RP, por sus siglas en inglés) alojado en la web que depende de un servicio de identidad en la nube, el Proveedor de Identidad (IDP, por sus siglas en inglés). En este caso, el RP puede ser una aplicación orientada al cliente o una aplicación orientada a la fuerza laboral;

- en un modelo de Sistema Único donde un archivo de sistema (el RP) provee control de accesos basado en la información del usuario recogida en el inicio de sesión (el IDP). En este caso, tanto el archivo de sistema como la función IAM están encapsulados en un sistema operativo.

---

gestión de identidades — Parte 2: Arquitectura de referencia y requisitos," https://www.iso.org/standard/57915.html (consultados el 28 de novembre de 2022).

[3] "Manual de Estrategia FICAM – Arquitectura FICAM – Ejemplos de Componentes de Sistema," Políticas generales de la División de Garantía de Identidades y Accesos fiables de la Administración de Servicios Generales (GSA, por sus siglas en inglés) https://playbooks.idmanagement.gov/arch/components/ (consultado el 28 de noviembre de 2022).

[4] Hazelton, Keith "La arquitectura de referencia TAP" https://spaces.at.internet2.edu/pages/viewpage.action?pageId=98306902 (consultado el 28 de noviembre de 2022).

[5] Grassi, Paul A., Michael E. Garcia, James L. Fenton, "Publicación especial NIST 800-63-3: Pautas de identidad digital" Instituto Nacional de Estándares y Tecnología, Departamento de Comercio de los Estados Unidos, junio de 2017, https://doi.org/10.6028/NIST.SP.800-63-3.

[6] Rose, Scott, Oliver Borchert, Stu Mitchell, Sean Connelly, "Publicación especial de NIST 800-207: Arquitectura de confianza cero" Instituto Nacional de Estándares y Tecnología, Departamento de Comercio de los Estados Unidos, agosto de 2020, https://doi.org/10.6028/NIST.SP.800-207.

[7] Hutchinson, Steve, "Introducción a la Identidad Parte 2 - 25 de junio" Identiverse 2019, a partir del minuto 27:39 de la grabación, https://www.youtube.com/watch?v=zxKRUXmTLJs&list=PLpKq7xRiIHaTDwAqpIU1UYpKZY03tfTMf&index=8.

Terminología

A continuación, se encuentran las definiciones de los términos. Aquellos marcados con un ✓ son los componentes abstractos comprendidos en el modelo.

Para facilitar la comprensión, los términos IDM y Administración del Acceso se utilizan como agrupaciones conceptuales de componentes.

Ítem	Definición
Control de Acceso	Los diversos métodos para limitar el acceso a datos, sistemas, servicios, recursos, ubicaciones de usuarios, un dispositivo o cosa.
✓Gobernanza de Acceso (también llamada Gobernanza y Administración de las Identidades (IGA))	La Gobernanza de Acceso provee vigilancia y control sobre los derechos de acceso implementados en múltiples sistemas de autorización locales o compartidos. Estos derechos pueden ser controlados de varias formas, comenzando por la existencia o validez de la identidad digital. Existen otros tipos de mecanismos de control como las políticas, el mapeo de roles, los permisos y las identidades. El concepto se abrevia IGA por las siglas en inglés para "Gobernanza y Administración de Identidades" y se utiliza mucho en el sector comercial. En términos generales, se corresponde a la sección "Certificación de Acceso" del componente de primera clase de los Sistemas de Gobernanza del modelo FICAM. IGA no está específicamente abordado en el modelo ISO/IEC.
✓Gestión de Acceso	Son los procesos y las técnicas utilizados para controlar el acceso a recursos. Esta capacidad trabaja junto con la Administración de Identidades y los terceros confiables para concretar su objetivo. En el modelo, la gestión de acceso es un conjunto de conceptos que reúne la función de Gobernanza de acceso y el componente de autorización compartido. Dicho esto, la gestión de acceso también impacta sobre la autorización local (a través de la función de gobernanza).
Aserción	Un mensaje formal o *token* que transmite información sobre una entidad, normalmente incluye un nivel de seguridad sobre un evento de autenticación y algunas veces incluye información adicional sobre atributos. También se le llama *Token* de Seguridad.
Nivel de Seguridad	Una categoría que describe la fortaleza del proceso de demostración de la identidad y/o el proceso de autenticación. Para más información, vea NIST SP.800-63-3.
✓Proveedor de Atributos	Cuando la autoridad para los atributos se diferencia de la autoridad para las identidades, el término que se usa es "Proveedor de Atributos". Es un subconjunto o un tipo de Autoridad de Información de la Identidad.
✓Repositorio de Auditoría	Es un componente que almacena registros de todo evento que pueda luego ser útil para determinar si las operaciones están acordes con la política, para apoyar investigaciones forenses y para permitir el análisis de patrones. Normalmente están altamente controlados para prevenir cualquier falsificación. Un repositorio de auditoría es el nombre ISO que se da a este concepto y forma parte del Administrador de Identidades (IDM, por sus siglas en inglés). En este modelo, el término está generalizado para referirse a cualquier servicio que apoye el registro de eventos desde cualquier parte del ecosistema.

✓Authenticación (AuthN)	El acto de determinar que a cierto nivel de seguridad el sujeto/entidad es auténtico.
Aserción AuthN	Es un *token* de seguridad en el que el Proveedor de Identidades provee información de seguridad y autenticación de forma segura al tercero confiable.
Autorización (AuthZ)	La autorización es cómo se toma una decisión durante la ejecución para permitir el acceso a un recurso. Se divide en dos tipos: compartidas y locales. El marco metodológico FICAM incluye a la misma como un subcomponente del Sistema de Administración de Acceso. El concepto AuthZ no está incluido en los modelos ISO ni Internet2.
✓AuthZ Compartida	Una autorización compartida es provista por fuera del RP. Aquí se muestra como parte de la gestión de acceso.
✓AuthZ Local	Una autorización local que es gestionada por el RP.
Credencial	Una credencial permite la autenticación de una entidad enlazando la identidad a un autenticador.
✓Proveedor de Servicios de Credenciales (CSP, por sus siglas en inglés)	Siguiendo la guía incluida en NIST 800-63-3, agrupamos bajo el nombre “Proveedor de servicios de credenciales" tanto la función de registro/inscripción como los servicios de credenciales.
Servicios de Credenciales	Los Servicios de Credenciales expiden o registran a los autenticadores inscriptos, entregan la credencial para usar y consecuentemente administran dichas credenciales. Incluimos información de infraestructura de clave pública (PKI, por sus siglas en inglés) para arquitecturas de Administración de Identidades y Accesos (IAM, por sus siglas en inglés) que deben incluir componentes del sistema que requieran certificados y claves privadas. En líneas generales, esto se corresponde al componente FICAM llamado Sistemas de Administración de Credenciales.
Cumplimiento	Son los mecanismos que aseguran que un individuo no pueda ejecutar una acción o acceder a un sistema cuando los mismos estén prohibidos por políticas.
Inscripción	La inscripción o registro concierne los aspectos de demostración y ciclo de vida del sujeto. La entidad que lleva a cabo la inscripción es a veces conocida como Autoridad de Registro, pero nosotros, conforme a NIST SP.800-63-3, utilizaremos el término Proveedor de Servicios de Credenciales.
Derechos	Artefacto que permite el acceso a un recurso por parte de una entidad principal. Se conoce también como privilegio, derecho de acceso, permiso o autorización. Un derecho puede ser implementado de muchas formas.
✓Autoridad de Información de Identidades (IIA, por sus siglas en inglés)	Representa una o más fuentes de datos usados por la Administración de Identidades (IDM, por sus siglas en inglés) como base para el conjunto maestro de registros de identidades de entidades principales o sujetos. Cada IIA puede proveer un subconjunto de registros y de atributos. A veces la IIA se diferencia del Proveedor de Información de Identidades o IIP. La IIA se usa para incluir el servicio que de hecho provee la información, así como la autoridad raíz. Esto se corresponde a “Fuente de Información de Identidades” en ISO/IEC 24760-2 y a “Fuentes de Identidades” en Internet2.

✓Administración de Identidades (IDM, por sus siglas en inglés)	Es un conjunto de políticas, procedimientos, tecnología y otros recursos usados para mantener la información de identidades. La IDM contiene información sobre entidades principales/sujetos, incluyendo credenciales. Puede también incluir otros datos como metadatos para habilitar la interoperabilidad con otros componentes. La IDM se muestra con una línea punteada para indicar que es una agrupación conceptual de componentes y no un sistema en sí mismo.
Proveedor de Identidades (IDP, por sus siglas en inglés)	Un Proveedor de Identidades o IdP es un término común. Lo consideramos un subconjunto de servicios dentro de la Administración de Identidades. Consiste en las interfaces de servicios: AuthN/Aserción, Agentes de Aprovisionamiento de Servicios, Administración de Sesiones, Servicios de Detección y Administración de Metadatos.
✓Registro de Identidad	Es un almacén de datos que contiene las entidades inscritas o registradas y sus correspondientes atributos, incluyendo sus credenciales. Vea la sección IDM para más detalles. Los términos Directorio, Repositorio de Identidad y Almacén de Atributos se utilizan frecuentemente como sinónimos.
✓Administración de Metadatos	Son los procesos y técnicas que permiten recopilar, utilizar y eventualmente eliminar los datos de control usados por la IDM para reconocer y confiar en el *Relying Part*y (o tercero confiable). El término se corresponde con "Datos del *Relying Party*" utilizado en el modelo Internet2.
✓Terceros Confiables (RP, por sus siglas en inglés)	Es un componente, sistema o aplicación que usa el Proveedor de Identidades (IdP, por sus siglas en inglés) para identificar a sus usuarios. El RP tiene sus propios recursos y lógica. Nótese que el término "servicio de confianza" (*relying service*) es utilizado en los estándares ISO/IEC para abarcar todos los tipos de componentes que usan servicios de identidad, incluyendo sistemas, subsistemas y aplicaciones, independientemente del dominio u operador. Aquí usaremos el término "terceros confiables" (RP) de la manera que es más comúnmente empleada. A grandes rasgos, un RP se corresponde con el término "*Agency Endpoint*" del modelo FICAM o con el término "Consumidores de Identidad" en el modelo Internet2.
✓Contexto de Riesgos (RCTX)	El Contexto de Riesgos es la información adicional que pueda ser aportada para ayudar a mejorar la seguridad general del ecosistema. Los eventos internos o externos y datos se pueden usar para habilitar, limitar o terminar el acceso. Este término es similar a la sección de Monitores y Sensores de los Sistemas de Gobernanza FICAM así como a varias de las entradas del Punto de Decisión de Políticas en la Publicación Especial 800-207 de NIST, un documento sobre Confianza Cero (*Zero Trust*).
Sesión	El período de tiempo que se inicia luego de un evento de autenticación, cuando un tercero confiable (RP) otorga acceso a recursos para el sujeto o entidad principal. La duración de la sesión y los mecanismos para su ejecución varían según la implementación.
✓Administración de Sesiones	Una función de administración provista por un Proveedor de Identidades (IdP) para controlar las sesiones de terceros confiables (RP) suscritos.
Marco de Confianza	Es un componente que representa el aparato legal, técnico y organizacional que habilita la confianza entre la IDM y los RP.
✓Raíz de Confianza	Es una estructura técnica que otorga a los IdP y los RP, la habilidad de reconocerse mutuamente a un nivel alto de seguridad. Es similar al concepto de Ancla de

	Seguridad (*Trust Anchor* / NIST SP.800-63-3) salvo que nosotros también incluimos en la definición a cualquier estructura que confíe en un tercero en el marco de un mutuo acuerdo. La Raíz de Confianza deriva de la ejecución de un Marco de Confianza.

Estructura básica del modelo

La función más básica de un sistema de identidad es proveer un almacenamiento seguro de la información de identidad y una forma para que los Terceros Confiables (RP) puedan usar esa información para controlar el acceso a recursos. El siguiente diagrama muestra los componentes principales de un sistema de administración de identidades (IDM) que soporta varios RP.

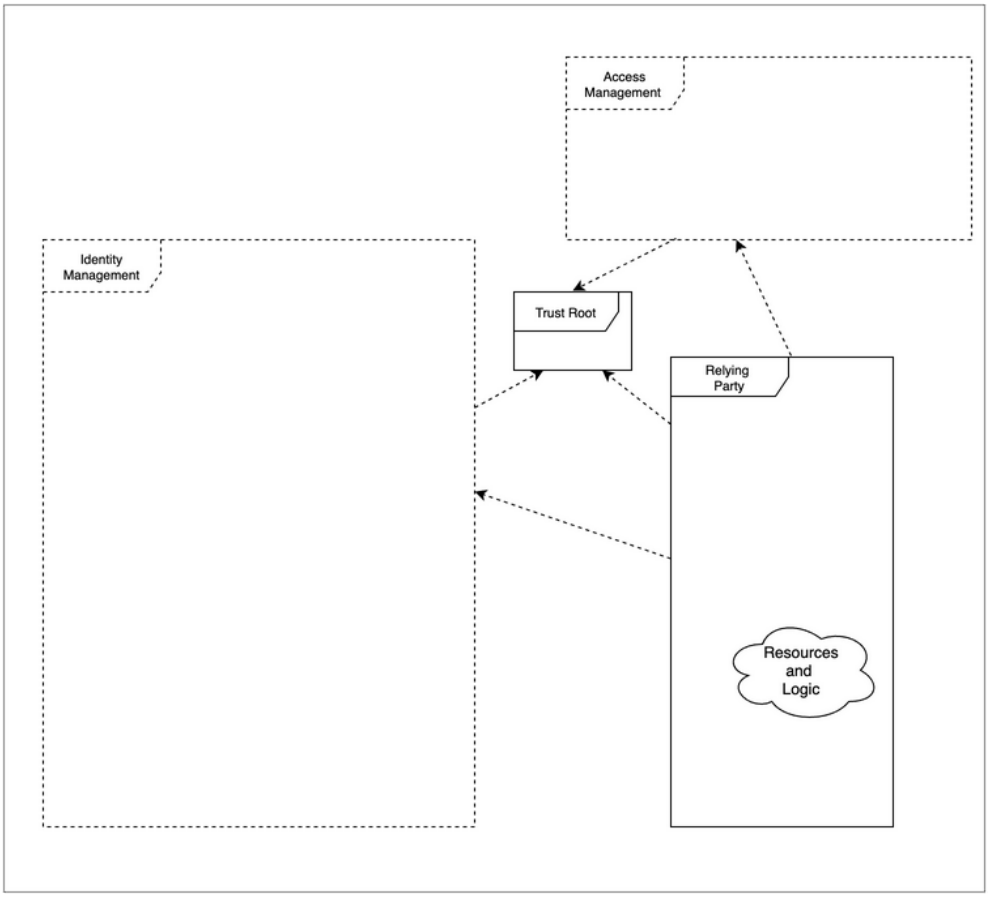

Figura 1: Dependencias fundamentales entre los componentes en un IDM que soporta varios terceros confiables. Los componentes principales del IDM se muestran aquí. Las líneas punteadas muestran las dependencias.

Administración de Identidades

La Administración de Identidades (IDM) es un conjunto de políticas, procedimientos, tecnología y otros recursos necesarios para mantener información de identidad. Este modelo contiene información sobre entidades/sujetos, incluyendo las credenciales.

También encontrarás información sobre los metadatos que habilitan la interoperabilidad con otros componentes. El IDM se muestra con una línea punteada para indicar que es un agrupamiento conceptual de componentes y no un sistema hecho y derecho en sí mismo.

Terceros Confiables

Los Terceros Confiables (RP) son un componente, sistema o aplicación que el IDM usa para identificar a sus usuarios. El RP tiene sus propios recursos y lógica. Viene en muchas formas, todas las cuales usan servicios de identidad incluyendo sistemas, subsistemas y aplicaciones independientes del dominio u operador.

Marco de Confianza

Este componente representa el aparato legal, organizacional y técnico que habilita la confianza entre el IDM y los RP.

El Marco de Confianza ocupa un rol fundamental cuando el IDM y el RP no están en la misma organización ya que ello implica acuerdos multilaterales o bilaterales. En casos simples, puede ser sencillamente un contrato entre dos partes. En otros casos, puede haber un acuerdo multilateral. Utilizaremos el término federación de manera amplia para referirnos a ambos casos. Estos marcos están descritos en profundidad en Leyes Regulatorias de Sistemas de Identidad (v2).[8]

Estos acuerdos, reglamentaciones y políticas rigen cómo operan e interactúan los miembros de una federación. [9] Para funcionar correctamente, las partes de una federación establecen acuerdos mutuos respecto a qué se considera una identidad aceptable. Esto se utilizará entre las partes que están en una relación federada (por ejemplo, se decide el nivel de seguridad que se aplicará). Asimismo, la definición y los valores de los atributos federados deben ser acordados. En una relación federada, las partes deben acordar las políticas de seguridad/acceso de los usuarios federados de ambas partes. Por ejemplo, en casos de fallas en la seguridad está el deber de avisar a las otras partes.

Cuando el IDM y el RP están en la misma organización, los acuerdos son más tácitos.

Cuando el IDM y el RP fueron creados en una misma infraestructura de sistema que habilita una confianza mutua, la misma puede ser opaca para el operador de sistema aunque el desarrollador del sistema conocerá el marco de confianza o al menos sus

[8] Smedinghoff T. J., (2021) "Las leyes que gobiernan a los Sistemas de Identidad (v2)," *Cuerpo de Conocimiento de IDPro Body of Knowledge* 1(5). https://bok.idpro.org/article/id/8/.
[9] Temoshak, David, Christine Abruzzi, "NISTIR 8149 - Desarrollo de marcos de confianza para admitir federaciones de identidad" Instituto Nacional de Estándares y Tecnología, Departamento de Comercio de los Estados Unidos, enero de 2018, https://doi.org/10.6028/NIST.IR.8149.

implicaciones ya que habrá tenido que implementar mecanismos que sustenten dicha confianza.

Raíz de Confianza

La raíz de confianza es una estructura técnica que otorga al IDP y al RP la capacidad de reconocerse mutuamente con cierto grado de certeza. Es similar al concepto de Ancla de Confianza (NIST SP.800-63-3) salvo que nosotros permitimos que una estructura confíe en un tercero que haya sido mutuamente acordado. Una raíz de confianza deriva del funcionamiento de un Marco de Confianza. Para que los sistemas puedan funcionar sin tener que involucrar a un humano en cada transacción, la raíz de confianza es necesaria. Esto puede realizarse mediante una Infraestructura de Clave Pública (PKI, por sus siglas en inglés), donde las partes acuerdan confiar en una autoridad de certificación común que firma los certificados de todas las partes de la federación. Esto puede hacerse mediante un conjunto de certificados independientes en los que las partes acuerdan confiar.

Aprovisionamiento

El aprovisionamiento es un término que abarca los procedimientos y métodos que crean, modifican y eventualmente eliminan una identidad y la información de perfil usada por la infraestructura TI y las aplicaciones de negocio. Mediante estos métodos se crean o actualizan los registros en el registro de identidad o se eliminan de este último. Con frecuencia, el aprovisionamiento debe extenderse a aplicaciones para apoyar decisiones de autorización. A veces se le conoce como “aprovisionamiento *downstream*”. El término “*Onboarding*” se utiliza algunas veces para referirse a la suma de las actividades iniciales de aprovisionamiento tanto en aspectos de identidad como de acceso.

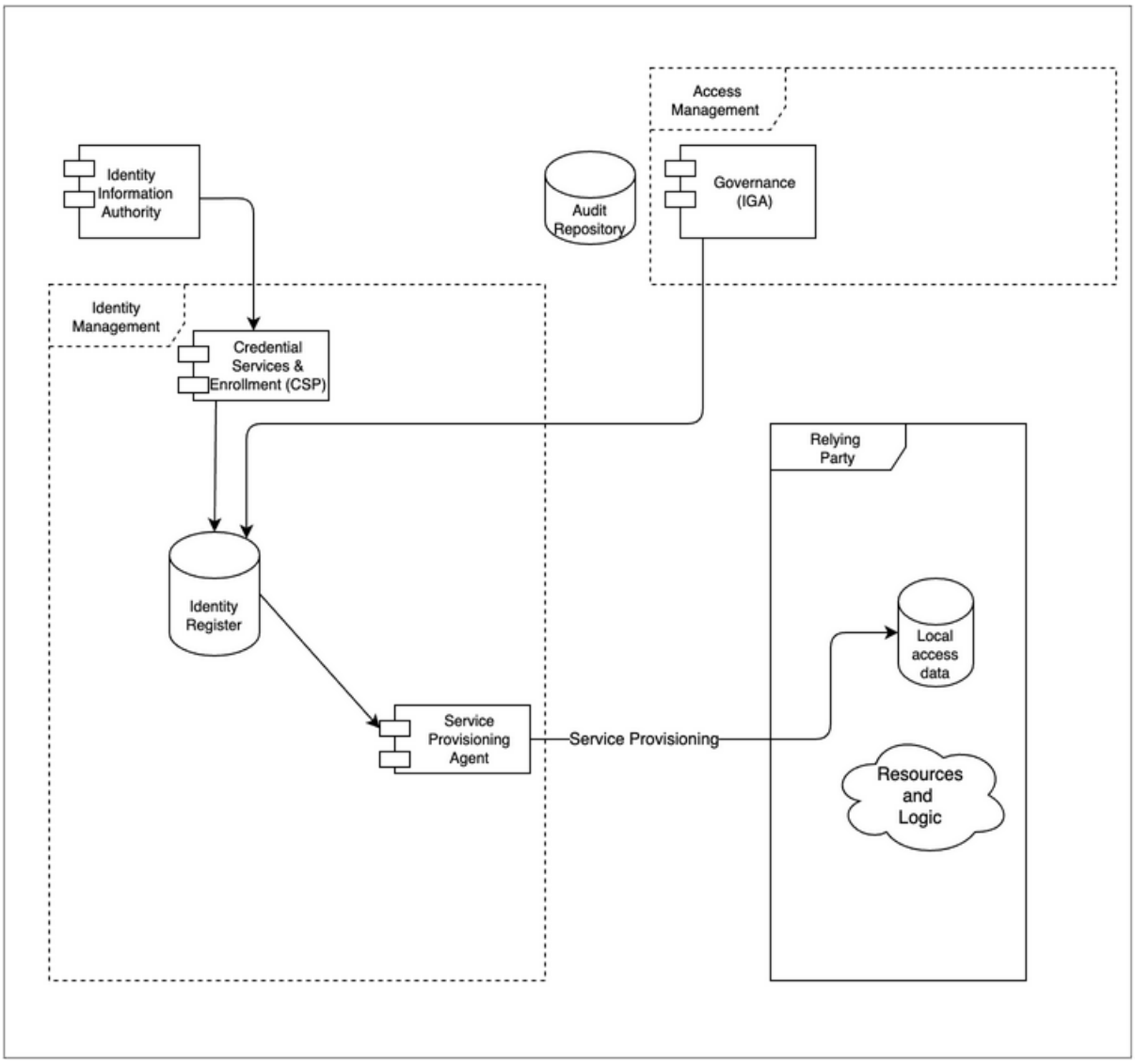

Figura 2: Aprovisionamiento: El registro de la identidad recibe actualizaciones de una o más fuentes externas y las acciones administrativas correspondientes y pasa la información a medida que sea necesaria.

Autoridades de información de identidad

Si bien es posible tener un IDM poblado sin anexarlo a un servicio de datos externo, generalmente esto no ocurre. Habitualmente, información de empleados o clientes debe ser importada. Podemos llamarlo “aprovisionamiento *upstream*”. Ten en cuenta que las fuentes de autoridad de atributos de identidad trascienden el sistema de Recursos Humanos y pueden incluir un correo electrónico, teléfono, sistema de certificación de formación, etc. En algunos casos una empresa puede tener más de un sistema de recursos humanos.

Gobernanza

El acto de aprovisionamiento puede incluir determinada lógica que está idealmente modelada bajo la forma de gobernanza. En algunos casos, el sistema IGA se encarga de todas las tareas de aprovisionamiento (ver más abajo la sección Gobernanza de Acceso).

Servicios de credenciales e inscripción

Esta tarea comprende los pasos necesarios para originar y activar una identidad. También está relacionada con el mantenimiento regular de la misma, en tareas como el restablecimiento de contraseñas y la rotación de claves. Asimismo, incluye actividades administrativas y tareas de autoservicio.

Inscripción

También llamada Registro. Involucra tareas como la demostración, verificación o investigación y respaldo del registro, en caso de ser necesario. También es responsable de la entrega segura de credenciales. La inscripción culmina cuando un usuario recibe formalmente la propiedad de su identidad digital y asume el control y posesión de las credenciales de su cuenta.

Servicios de credenciales

Los servicios de credenciales incluyen la creación de contraseñas, claves criptográficas y otros autenticadores. Los asocia o “vincula” a un registro de identidad. También se encargan del mantenimiento regular como el restablecimiento de contraseñas, la rotación de claves y la revocación de credenciales, en caso de que sea necesario.

Registro de la identidad

Es un almacén de datos que contiene las entidades registradas y sus atributos, incluyendo sus credenciales. En este modelo haremos de cuenta que estamos en una base de datos única. En la práctica, los diseños pueden almacenar algunos atributos separadamente de las identidades. También utilizamos el término de manera que abarque el almacenamiento de credenciales, aunque todas o algunas de las credenciales pueden estar almacenadas en su propio repositorio físico.

Por su naturaleza, se requiere que los registros de identidad tengan alta disponibilidad. Con frecuencia, a nivel físico, los registros contienen varias instancias que se sincronizan. El Registro de Identidad puede implementarse de varias maneras. Algunos de los métodos más comunes incluyen la utilización de bases de datos de uso general y de almacenes optimizados como directorios físicos o virtuales.

Importar datos no significa necesariamente hacer una copia física de los datos, aunque muchas veces se hace. El término también abarca la idea de virtualización, donde la importación de información de identidad se realiza durante la ejecución.

Servicio de agente de aprovisionamiento

A veces, hay una necesidad de llevar cierta información selecta más lejos dentro del ecosistema. Habitualmente esto ocurre cuando un RP necesita información adicional sobre los usuarios para controlar el acceso o con fines de personalización. El RP hace una copia de la información de identidad para usarlos a futuro en los procesos de la aplicación. Una solución completa debería mantener el ciclo de vida completo de la información, incluyendo la creación, actualización y eventual eliminación de la información de la identidad almacenada localmente.

Aprovisionamiento justo-a-tiempo

Hasta ahora hemos abordado las tareas de aprovisionamiento enfocándonos en el “tiempo de administración”. Sin embargo, en algunos casos el aprovisionamiento ocurre durante la ejecución.

Si bien no lo mostraremos aquí, algunas veces las acciones de aprovisionamiento ocurren de forma “justo-a-tiempo”. Esto puede suceder cuando información de identidad adicional es pasada a un RP en tiempo real para dar respuesta a un requisito específico de una aplicación, incluyendo probablemente atributos de identidad (ver Autenticación y Sesiones). Un caso similar ocurre cuando el RP solicita al IDM que obtenga atributos (ver Autorización más adelante en el documento).

Repositorio de auditoría

El repositorio de auditoría muestra la acumulación de eventos de datos históricos. Para evitar confusiones, asumiremos que la información de autoría es escrita, pero la representamos con flechas en el diagrama.

Autenticación y sesiones

Autenticación

La autenticación es el procedimiento mediante el cual las credenciales de un sujeto son usadas para verificar su identidad. El IDP verifica las credenciales que se le presentan. Existen varios escenarios posibles. Típicamente, el RP solicita al Proveedor de identidad que recoja las credenciales del usuario y recibe una evaluación por parte del IDP sobre el nivel de certeza que tiene de que el usuario es auténtico. Seguidamente, la evaluación (e información adicional sobre el usuario) es entregada el RP a través de un token de seguridad protegido criptográficamente. Existen muchas variedades de tokens de

seguridad. El diagrama utiliza flechas bidireccionales para mostrar que existen casos de uso que requieren intercambios de información continuos tal y como describimos en la sección de este documento llamada “Sesiones”.

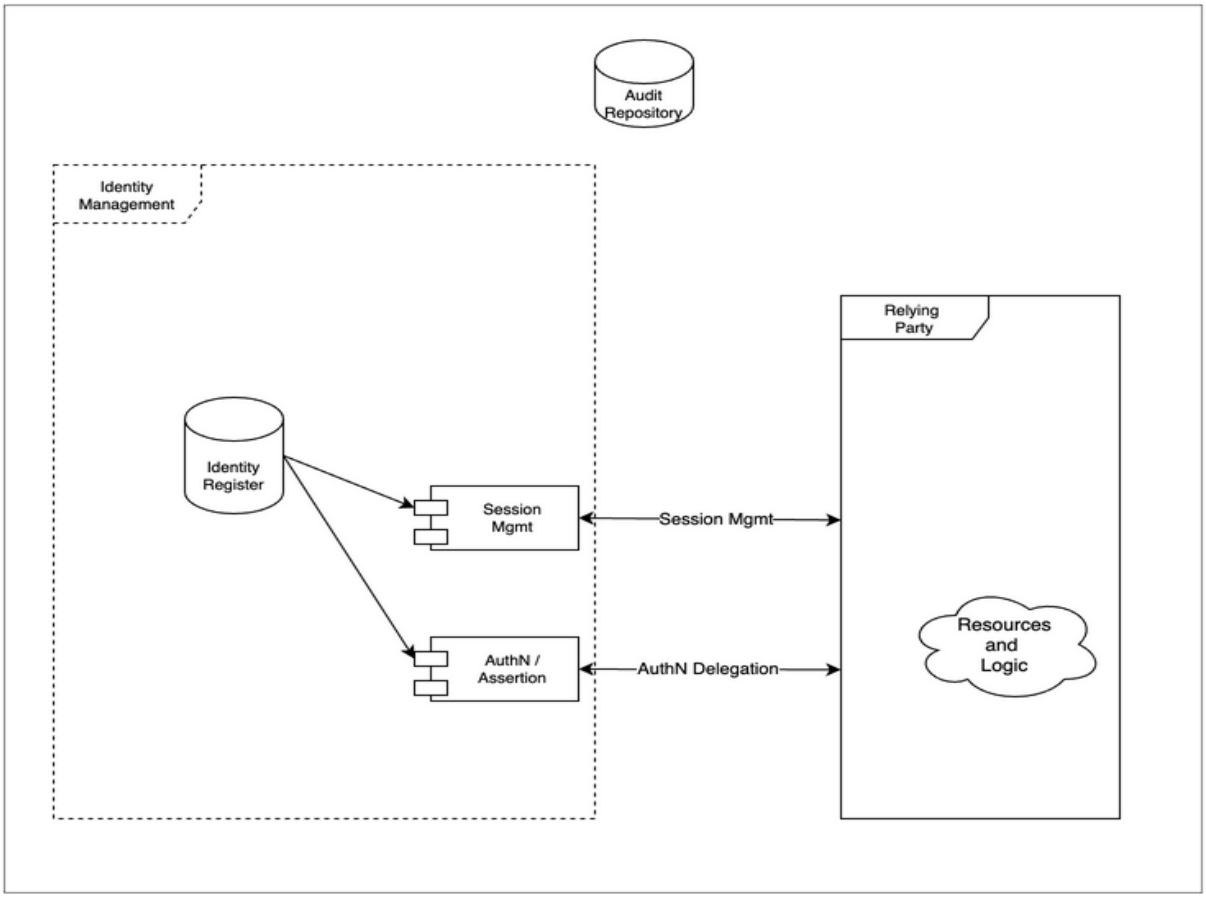

Figura 3: Autenticación y Sesiones: El Registro de la Identidad da soporte a los escenarios de autenticación. El IDP puede monitorear o participar en la totalidad del ciclo de vida de la sesión con los terceros confiables.

Sesiones

Es común que se asocie el evento de autenticación con el comienzo de una sesión. La sesión es un asunto que concierne al RP. Sin embargo, a veces es deseable tener sincronizadas las sesiones de varios terceros confiables para que, por ejemplo, al desloguearse de una sesión se cierren todas las sesiones simultáneas. En general, es el IDP quien orquesta el cierre de sesiones. En entornos de alta seguridad, la gestión de sesiones debe admitir el cierre de sesión basado en información de la identidad en tiempo real, como en casos en los que los derechos de un usuario han sido modificados.

Un punto de vista centralizado de las sesiones es útil para aplicar buenas prácticas de seguridad. Por ejemplo, si los atributos de identidad de un usuario con una sesión activa

cambian y los nuevos valores desobedecen una política de control de acceso, la sesión debe terminarse. Si la administración de sesiones está al tanto de una cuenta terminada, debe terminar cualquier otra sesión activa del usuario. Esto puede ocurrir también en escenarios avanzados en los que monitores de riesgos externos expongan eventos de este tipo. Ver la sección Contexto de Riesgos más abajo.

Las sesiones también involucran otro concepto importante: la autenticación incremental. Una sesión puede dar seguimiento al nivel de garantía de una autenticación particular de modo que cuando un usuario solicita acceso para realizar una transacción o para acceder a una aplicación que requiere un nivel de garantía de la identidad más alto, el IDP estará preparado para determinar qué camino seguir, como por ejemplo decidir aumentar la certeza de que el usuario es la persona correcta solicitándole que provea evidencia adicional. Por ejemplo, es posible que la contraseña sirva para revisar parte de la información, pero para retirar dinero se requiere de un factor adicional como una contraseña de un solo uso de una aplicación móvil. La detección de una brecha de seguridad y su consiguiente acción será lógicamente realizada en el RP pero para evitar una experiencia de usuario pobre en múltiples escenarios de RP, se debe registrar la autenticación incremental en la sesión.

Autorización

Existen muchos y variados modelos de autorización. El diagrama ilustra dos abordajes de la autorización: local y compartida. Como se ve abajo, ambos abordajes están sujetos a la Gobernanza de Accesos.

Típicamente, ambos abordajes utilizan atributos del sujeto para determinar el acceso, aunque algunos sistemas se basan en enumeraciones directas que asocian usuarios a recursos, conocidas como listas de control de acceso.

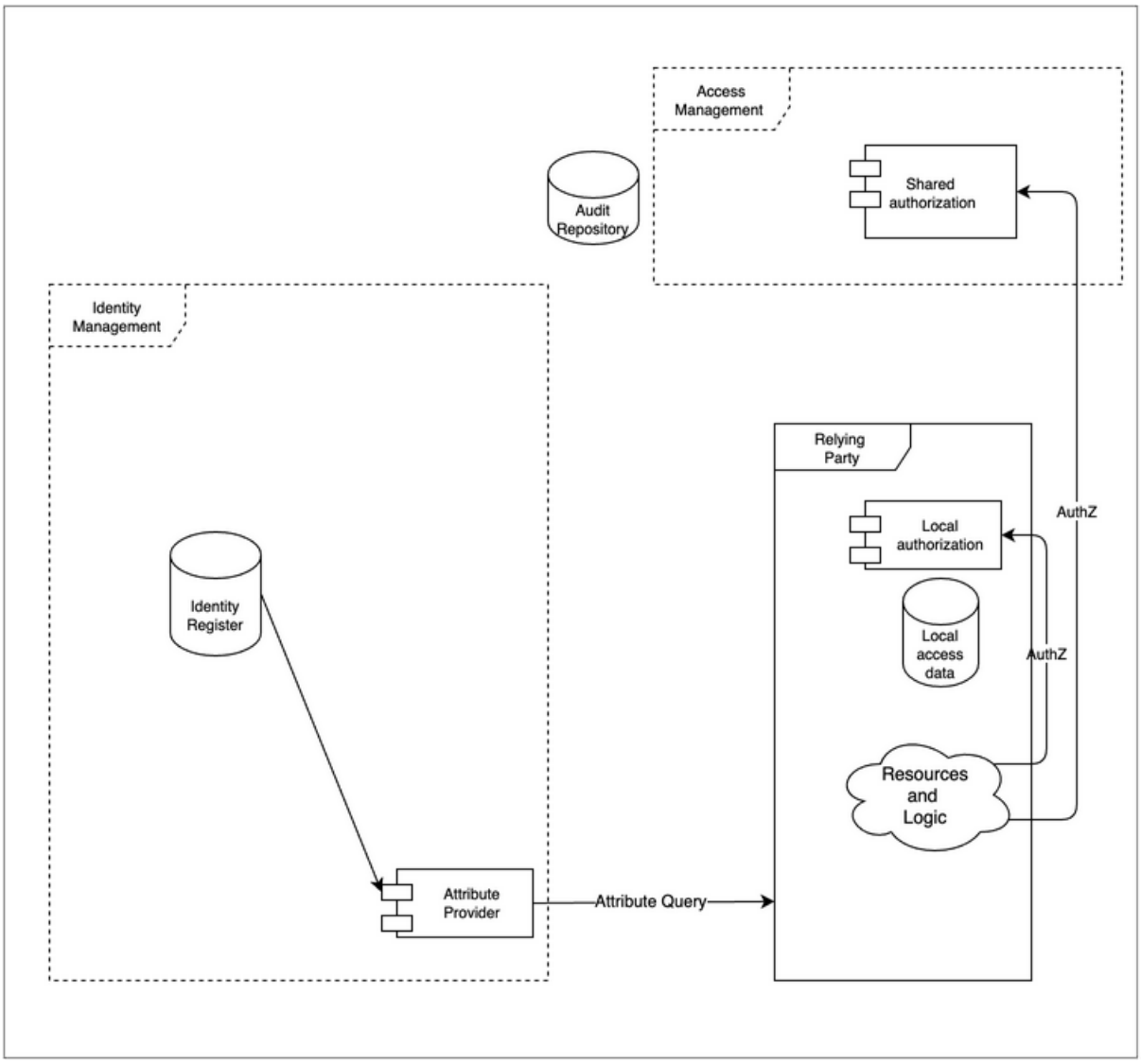

Figura 4: Modelos de autorización: Algunos RP realizan las tareas de autorización internamente. A veces la autorización es un recurso compartido por varios RP.

Autorización local

Los Terceros Confiables que realizan las tareas de autorización internamente son muchos. Con frecuencia ocurre que el control de acceso requerido por un recurso protegido es tan detallista que resulta tentador realizar las tareas de autorización internamente. Por ejemplo, un sistema de administración financiero puede mantener los derechos de un usuario para una funcionalidad específica dentro de la propia aplicación. En ese escenario, la aplicación toma la decisión de autorización e implementa (ejecuta) el resultado.

Los valores de control pueden haber sido provistos al almacén local de información de acceso mediante el proceso de aprovisionamiento descrito aquí arriba. Asimismo, los

valores pueden recogerse de la búsqueda de atributos del IDM durante la ejecución, proveyendo el rol del usuario u otros atributos que aparezcan en el inicio de sesión, quizás como un valor en el token de seguridad.

Autorización compartida

A veces una autorización es un recurso compartido entre varios terceros confiables. Dicho diseño aumenta la consistencia de las decisiones de autorización y da soporte a organizaciones que desean incorporar estrategias de decisiones de acceso avanzado como las requeridas por el método de control de accesos “Confianza Cero” (“Zero Trust”). Generalmente, los sistemas de autorización compartida tienen una aproximación consistente a las políticas, teniendo, por ejemplo, un lenguaje de políticas estandarizado. En este escenario, el RP solicita a la función de autorización compartida que tome la decisión, pero la implementa (ejecuta) él mismo.

Mecanismos de autorización

Cualquiera sea el abordaje, los derechos de acceso pueden establecerse, mantenerse y revocarse de varias maneras, comenzando por la existencia y validez de la identidad digital. Existen otros controles que incluyen una variedad de mecanismos como políticas, roles, permisos e identidades. Algunos controles se basan en los atributos del usuario, incluyendo la membresía a un grupo o roles almacenados en un Registro de Identidad. Algunos controles pueden depender de las propiedades del recurso accedido o del contexto de la solicitud, como la hora, el dispositivo o la ubicación.

Para implementar el control de accesos, cada mecanismo se basa en una estructura lógica de datos concreta. Esa estructura de datos es el foco de los implementadores. Por ejemplo, en un caso de control de acceso basado en roles se requiere de cierto arte para la “Gestión de Roles” (es decir la definición y administración de un conjunto de roles útiles), ya que demasiados roles son difíciles de gestionar, mientras que muy pocos conducen a tener usuarios con acceso a cosas que no necesitan. De manera similar, en el caso del control de acceso basado en políticas, el conjunto de políticas (las normas de la política) debe ser diseñado, almacenado y gestionado.

Gobernanza de Acceso

La Gobernanza de Acceso también conocida como Gobernanza y Administración de la Identidad (IGA), controla los derechos de acceso implementados en varios sistemas de autorización locales o compartidos. A menudo, esta tarea entra en juego en la administración de estos derechos y en la supervisión necesaria para garantizar a lo largo del tiempo que todo está en orden respecto a esos derechos.

En sistemas de empresa, la Gobernanza de Acceso se enfoca en gestionar los derechos del equipo de trabajo (empleados/contratistas). El concepto puede aplicar también a otros escenarios como cuando se requieren derechos administrativos delegados de una compañía negocio-a-negocio o en escenarios negocio-a-cliente donde terceras partes autorizadas, como abogados, son requeridas.

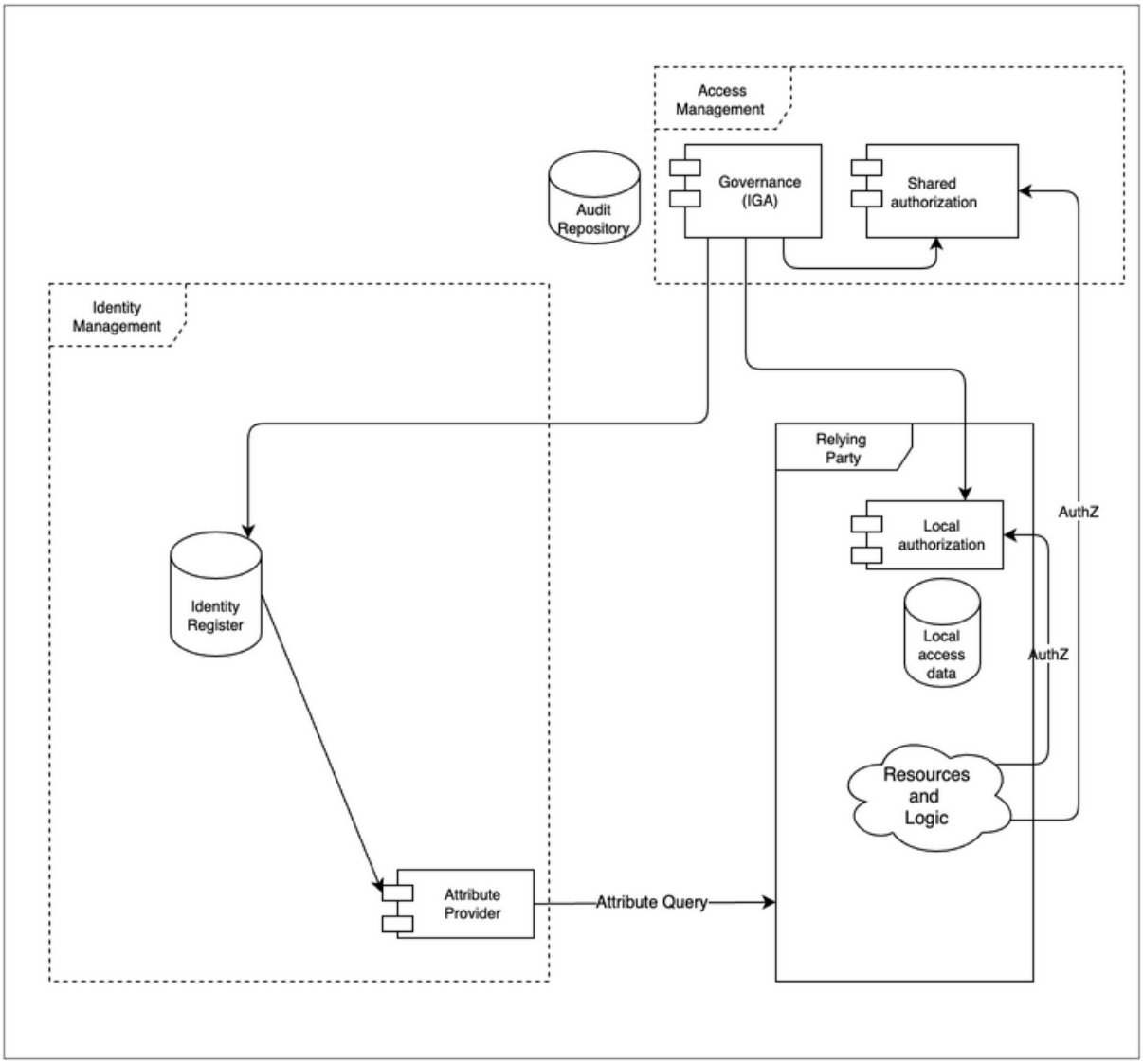

Figura 5: La Gobernanza de Acceso provee la supervisión y el control sobre los derechos de acceso implementados en varios sistemas de autorización locales y, a veces, en sistemas de autorización compartidos.

Control

Los controles pueden incluir métodos como procedimientos o procesos de trabajo que garanticen una correcta supervisión. Típicamente, una solicitud de acceso a recursos se pasa a una o más personas para que la aprueben y se crea un registro de auditoría.

Con el fin de prevenir fraudes internos la “separación de los deberes” se implementa frecuentemente. Este es un control que define grupos de derechos de acceso que no pueden ser poseídos por una misma persona. Idealmente, este control debe implementarse en una ubicación donde tenga visibilidad a todos los derechos de acceso implicados, por ejemplo, en un sistema IGA.

Supervisión

Típicamente, las actividades de gobernanza revisan y potencialmente modifican la información en uno o más componentes de autorización con el fin de efectuar un cambio en los derechos. Con frecuencia, las organizaciones tienen procedimientos formales para revisar los derechos existentes y pueden requerir de un tercero responsable para certificar o atestar que estos derechos están en orden. Otras herramientas para garantizar la efectividad de los controles de las políticas IAM incluyen auditorías internas y externas, así como informes analíticos.

Contexto de riesgo

La información de Contexto de Riesgo (a menudo abreviado como RCTX) puede ser valiosa para mejorar la seguridad del servicio en el que se está confiando. El riesgo puede evaluarse basándose en la información de la solicitud, en información del historial del usuario o en aserciones/evidencia proveniente de terceros.

La conexión que va del Repositorio de Auditorías al Contexto de Riesgo ilustra que este último puede hacer uso de la información local histórica sobre eventos.

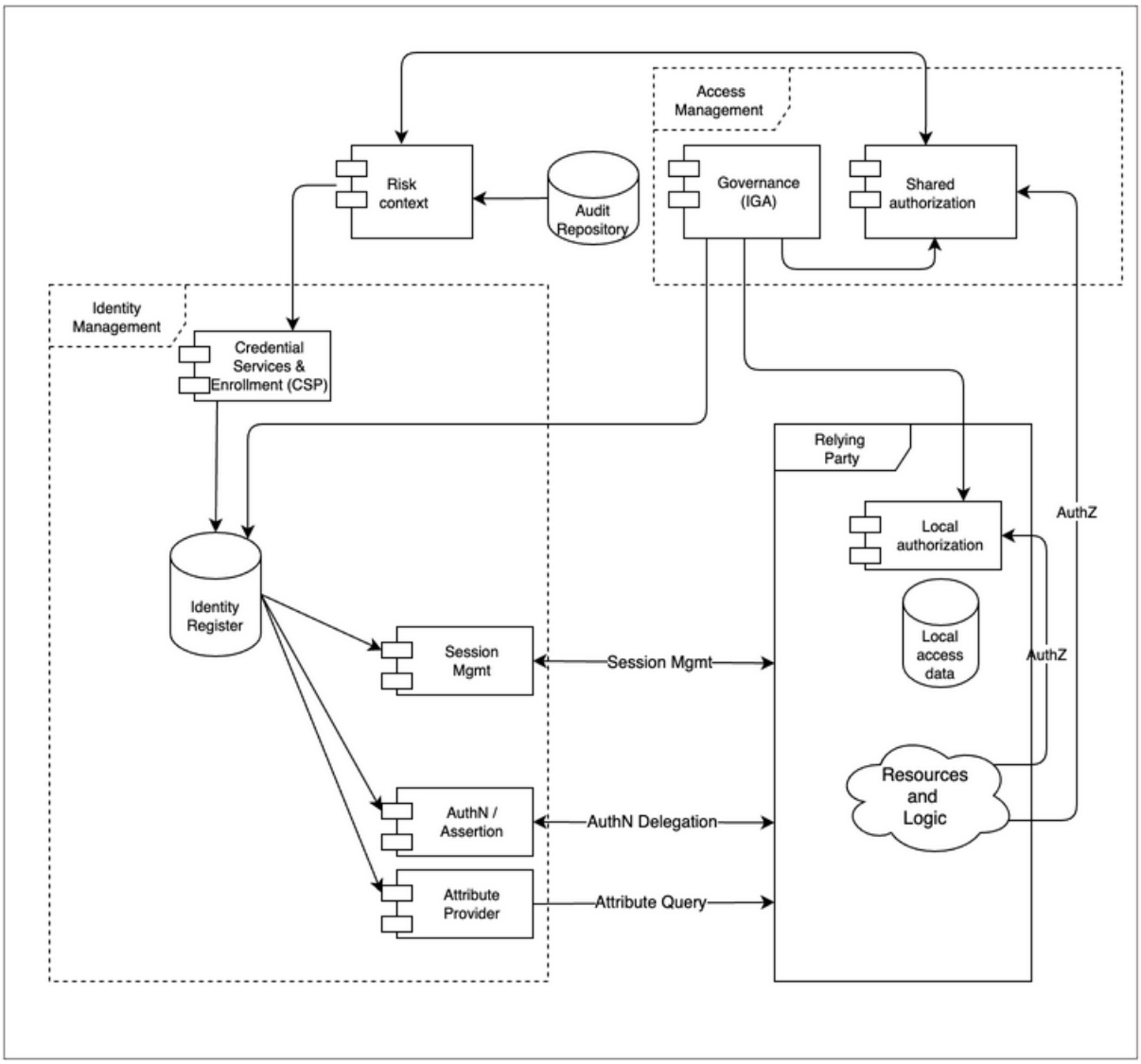

Figura 6: Contexto de Riesgo: es posible usar información de riesgo en decisiones de autenticación. Por ejemplo, si una contraseña robada se encuentra en la dark web, no permitas el acceso.

El operario IDM puede acceder a información sobre eventos externos adquiriendo paquetes de consorcio o de proveedores. En algunos escenarios de colaboración, es viable que el operario IDM divulgue los eventos de riesgo para el beneficio de otros, colaborando con el cumplimiento de los requisitos de administración de riesgos de otros operarios.

Para que el IDM pueda modificar el comportamiento de su función de autenticación, se le deben proporcionar los eventos de forma que pueda usarlos selectivamente. Por ejemplo, al contar con información adicional sobre eventos, la función de autenticación puede solicitar una autenticación incremental o directamente denegar el acceso.

En algunos escenarios graves, para que las sesiones actuales puedan ser revisadas y terminadas en caso de que sea necesario, es aconsejable adjuntar los eventos a la función

de administración de sesiones. El grupo de trabajo de Señales y Eventos Compartidos de *OpenID* está desarrollando formas estándares de entregar estas señales.[10]

Como muestra el diagrama, los sistemas de autorización compartida también pueden hacer uso de la información de riesgo. Por ejemplo, una autorización puede denegarse si el historial reciente de actividades del sujeto está por fuera de los límites normales, ya que esto podría indicar que una credencial está comprometida. Lógicamente esto podría pasar también con una autorización local, pero esto no está representado en el diagrama.

Ejemplo: Información en la solicitud

Control de límites

Una decisión de autenticación o autorización puede verse influenciada por criterios específicos como por ejemplo si la solicitud proviene de una red conocida o desconocida. Una versión más específica de esto es la prohibición del acceso desde determinados países.

Ejemplos: Uso histórico

Uso de la coincidencia de patrones

Determina si la solicitud está por fuera de los patrones de uso normal para un individuo determinado. La referencia del uso histórico de patrones habilita la detección de patrones y puede ayudar a establecer una medida de riesgo para un usuario, una transacción específica o en general. Esto se llama perfil de riesgos.

Violación de la política de *land speed*

Mejorar la solicitud del usuario y su historial con información sobre su ubicación permite identificar una cuenta posiblemente comprometida ya que un mismo usuario no puede estar en dos lugares al mismo tiempo.

En estos casos se depende de señales del ambiente local pero también es posible obtener señales más lejanas.

Ejemplo: Terceras partes

Determinar las contraseñas más comúnmente usadas es posible basándose en posteos en la "*dark web*" (o Internet oscura). Los actores maliciosos obtienen estas contraseñas con la esperanza de que los usuarios usen la misma contraseña en otros sitios.

[10] "Grupo de Trabajo de Señales y Eventos Compartidos – Visión general" https://openid.net/wg/sse/ (Consultado el 28 de noviembre de 2022).

Ante al caso de que una de estas contraseñas sea presentada, el operario IDM puede requerir una confirmación adicional por parte del usuario.

Metadatos y Descubrimiento

Los metadatos permiten controlar la información que necesitan los IDM y los Terceros Confiables para interoperar.

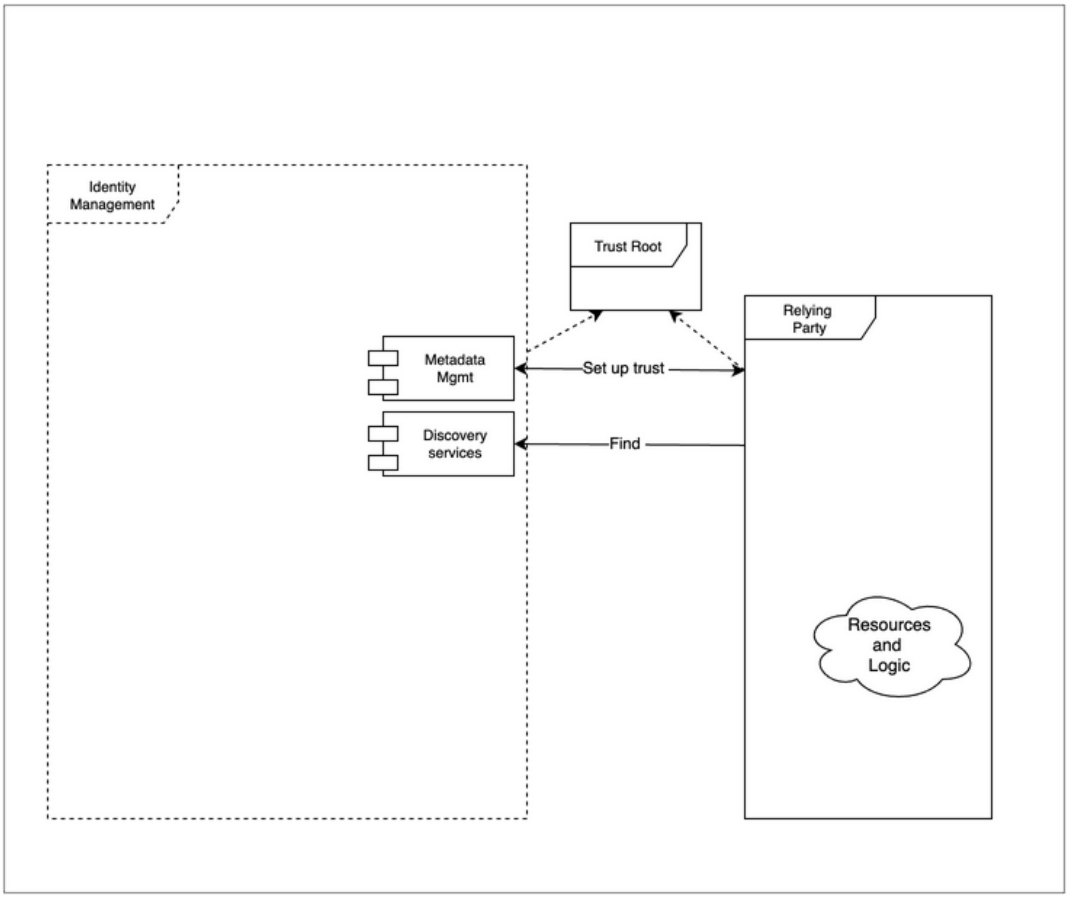

Figura 7: Metadatos y descubrimiento, estas dos funciones están involucradas en el reconocimiento mutuo entre el IDM y el Tercero Confiable.

Un ejemplo de esto es el registro de certificados de clave pública con el fin de permitir una autenticación mutua. En algunos escenarios, esta información se comparte manualmente entre las partes. Para validar el canal de seguridad (PKI) en sistemas distribuidos durante la ejecución, la raíz de confianza técnica es necesaria.

Otro ejemplo muestra que la información de configuración es otra forma de metadatos. *OpenID Connect* tiene una lista de valores requeridos, recomendados y opcionales que describen una implementación específica que apunta a proveer cierto grado de automatización durante la configuración.

Los metadatos pueden contener información que delimita los tipos de interacciones y el alcance de la información intercambiada. Asimismo, puede contener información de seguridad que permita que las contrapartes se autentiquen entre sí. Por ejemplo, se pueden usar componentes de clave pública como por ej. certificados emitidos por una misma autoridad.

El concepto de "Descubrimiento" hace referencia a los protocolos que facilitan la automatización. Por ejemplo, *OpenID Connect* define un método para que los Terceros Confiables ubiquen un *end-point* (punto final) donde la identidad de un usuario pueda ser verificada. [11] Este concepto es utilizado por otros métodos como SAML.[12] Un servicio de Descubrimiento puede aconsejar sobre dónde es mejor ubicar ciertos datos específicos para ser accedidos y sobre qué *end-points* se deben mantener para permitir que un RP use el servicio de identidad.

Biografía del Autor

George Dobbs dirige los arquitectos en una gran empresa aseguradora. Es también presidente del Comité del Cuerpo de Conocimiento de IDPro. Uno de sus intereses es la modernización del uso de las técnicas de Administración de Identidades y Accesos usadas por la firma. Le interesa particularmente el área de las aplicaciones orientadas al cliente, incluyendo abordajes para la prevención de fraude en contextos digitales y *call centers*. En relación con esto, le interesa también la evolución de la gestión de sesiones distribuidas - principalmente en la terminación de sesiones distribuidas. Es miembro fundador de IDPro y representó a su firma en el *Identity Ecosystem Steering Group* (IDESG). Previo a su posición actual, estuvo a cargo del desarrollo de aplicaciones de identidad orientadas al cliente en otras tres empresas aseguradoras. Desde el año 2004, condujo el grupo local de usuarios de administración de identidades y accesos. Anteriormente, fue presidente de *Network Applications Consortium*.

Agradecimientos

El autor quiere agradecer a Ian Glazer, Graham Williamson y Corey Scholefield por las minuciosas devoluciones de los primeros borradores; a Jon Lehtinen y Steve Hutchinson por algunas de las definiciones de su documento inédito "Introducción a la Identidad Parte 3"; y a Bertrand Carlier por su devolución tan rigurosa y atenta.

---

[11] Sakimura, N., J. Bradley, M. Jones, E., Jay, "OpenID Connect Discovery 1.0 que incorpora el conjunto de erratas 1" OpenID Foundation, 8 November 2014, https://openid.net/specs/openid-connect-discovery-1_0.html (Consultado el 28 de noviembre de 2022).

[12] Widdowson, Rod, Scott Cantor, "Protocolo y perfil del servicio de descubrimiento de proveedores de identidad" Especificción 01 del Comité OASIS, 27 de marzo de 2008, https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf (Consultado el 28 de noviembre de 2022).

Registro de cambios

Fecha	Cambio
30-09-2021	V1 publicada
15-12-2022	V2 publicada; cambios editoriales menores; algunas aclaraciones en el texto: en Servicios de Credenciales y en Autenticación.

Referencias

[1] Colaboradores de Wikipedia, "*All models are wrong*," *Wikipedia, La enciclopedia libre,* https://en.wikipedia.org/w/index.php?title=All_models_are_wrong&oldid=1111346950 (Consultado el 28 de noviembre de 2022).

[1] ISO/IEC 24760-1 *Second edition "IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts*," https://www.iso.org/standard/77582.html e ISO/IEC 24760-2, 2015 "*Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements*," https://www.iso.org/standard/57915.html (Consultado el 28 de noviembre de 2022).

[1] "*FICAM Playbooks – FICAM Architecture – System Component Examples*," *Identity Assurance and Trusted Access Division in the GSA Office of Government-wide Policy*, https://playbooks.idmanagement.gov/arch/components/ (Consultado el 28 de noviembre de 2022).

[1] Hazelton, Keith "*The TAP Reference Architecture (RA)*" https://spaces.at.internet2.edu/pages/viewpage.action?pageId=98306902 (Consultado el 28 de noviembre de 2022).

[1] Grassi, Paul A., Michael E. Garcia, James L. Fenton, "*NIST Special Publication 800-63-3 – Digital Identity Guidelines*," Instituto Nacional de Normas y Tecnologías, Departamento de Comercio de EE.UU., junio 2017, https://doi.org/10.6028/NIST.SP.800-63-3.

[1] Rose, Scott, Oliver Borchert, Stu Mitchell, Sean Connelly, "*NIST Special Publication 800-207 – Zero Trust Architecture*," Instituto Nacional de Normas y Tecnologías, Departamento de Comercio de EE.UU., agosto 2020, https://doi.org/10.6028/NIST.SP.800-207.

[1] Hutchinson, Steve, "*Introduction to Identity Part 2 – 25 de junio*," Identiverse 2019, grabación empieza en el minuto 27:39, https://www.youtube.com/watch?v=zxKRUXmTLJs&list=PLpKq7xRilHaTDwAqpIU1UYpKZY03tfTMf&index=8.

[1] Smedinghoff T. J., (2021) "*Laws Governing Identity Systems (v2),*" *IDPro Body of Knowledge* 1(5). https://bok.idpro.org/article/id/8/.

[1] Temoshak, David, Christine Abruzzi, "*NISTIR 8149 - Developing Trust Frameworks to Support Identity Federations*," Instituto Nacional de Normas y Tecnologías, Departamento de Comercio de EE.UU., enero 2018, https://doi.org/10.6028/NIST.IR.8149.

[1] "*Shared Signals and Events WG*" https://openid.net/wg/sse/ (Consultado el 28 de noviembre de 2022).

[1] Sakimura, N., J. Bradley, M. Jones, E., Jay, "*OpenID Connect Discovery 1.0 incorporating errata set 1*," *OpenID Foundation*, 8 de noviembre de 2014, https://openid.net/specs/openid-connect-discovery-1_0.html (Consultado el 28 de noviembre de 2022).

[1] Widdowson, Rod, Scott Cantor, "*Identity Provider Discovery Service Protocol and Profile*," Especificación 01 del Comité OASIS, 27 de marzo de 2008, https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf (Consultado el 28 de noviembre de 2022).