Föderiertes IAM – gemeinsam stärker

Annett Laube-Rosenpflanzer, Gerhard Hassenstein, Ronny Bernold

Unternehmen und Institutionen haben über Jahre hinweg geschlossene administrative Domänen für ihre IT-Systeme aufgebaut. Darin verwalten sie die digitalen Identitäten der eigenen Mitarbeitenden und externer Benutzerinnen und Benutzer (z.B. Kunden) sowie deren Zugriffsrechte für ihre verschiedenen Applikationen. Dies ist mit grossem administrativen Aufwand und hohen Kosten verbunden. Zumal nicht alle Organisationen über eine zentrale Benutzer- und Rechteverwaltung verfügen. Oftmals müssen die Zugangsdaten für jede Applikation einzeln gepflegt werden. Die Pflege und Verwaltung von Berechtigungsdaten ist eine ressourcenintensive Aufgabe. Das birgt neben dem erhöhten Fehlerpotenzial auch viele Sicherheitsrisiken. Föderierte IAM-Systeme, die es erlauben, Identitäten in mehreren Domänen zu verwenden, schaffen da Abhilfe. Sie bieten einfache Integration in vorhandene Systeme und die Wiederverwendung von existierenden Authentisierungsdiensten. So werden die Identitätsinformationen mitsamt ihren fortlaufenden Änderungszyklen beherrscht.

Prof. Dr. Annett Laube-Rosenpflanzer
Institutsleiterin ICT-based Management
Berner Fachhochschule
Technik und Informatik
annett.laube@bfh.ch

Prof. Gerhard Hassenstein
Dozent für Internet Security
Berner Fachhochschule
Technik und Informatik
gerhard.hassenstein@bfh.ch

Ronny Bernold
Co-Leiter B2.06
Berner Fachhochschule
E-Government-Institut
ronny.bernold@bfh.ch

Das grundlegende Ziel einer Identitäts- und Zugriffsverwaltung (engl. Identity and Access Management, IAM) ist es, den Zugriff von Subjekten (natürlicher Person, Organisation oder Service) auf Ressourcen (Anwendung, Service oder Daten) zu kontrollieren. IAM ermöglicht so die individualisierte Bereitstellung von Ressourcen. Heute gehört IAM zu den Standardsicherheitskonzepten in der IT, und es existieren viele funktionierende Lösungen. Das Spektrum reicht von einfachen Benutzerverwaltungen, bei denen einem Benutzerkonto, bestehend aus Benutzername und Passwort, Berechtigungen oder Rollen zugeordnet werden, bis zu unternehmensübergreifenden Verzeichnisdiensten, die ein Single Sign-on ermöglichen.

Bestandteile eines IAM

Konzeptionell besteht ein IAM aus drei Ebenen: IAM steuern, IAM definieren und Zugriff kontrollieren (siehe Abbildung 1)[1]. Die IAM-Steuerung beschreibt die Definition der notwendigen Vorgaben und Rahmenbedingungen für den Betrieb der Umgebung. Beim Definieren des IAM werden Subjekten, meist Personen, digitale Identitäten (E-Identity) zugeordnet und die entsprechenden Berechtigungen auf die Ressourcen verwaltet. Hier werden alle notwendigen Bedingungen geschaffen, damit zur Ausführungszeit bestimmt werden kann, ob ein Subjekt auf eine Ressource zugreifen darf. Ziel der Zugriffskontrolle ist die kontrollierte und garantierte Einhaltung der Regeln für den Zugriff eines Subjekts auf eine Ressource.

Anders ausgedrückt besteht ein IAM aus einem Identitäts- und einem Zugriffsmanagement. Das Identitätsmanagement bildet das Subjekt in einer maschinenlesbaren E-Identity ab. Ein Subjekt kann dabei mehrere Identitäten besitzen, zum Beispiel für verschiedene Anwendungen. Eine digitale Identität besteht aus einem Identifikator (im einfachsten Fall einem Benutzernamen) und einer Menge personenbezogener Attribute. Der Identifikator wird zusammen mit geeigneten Credentials vom Subjekt benutzt, um sich an einem System zu authentisieren. Das Identitätsmanagement ist die Voraussetzung für das Zugriffsmanagement. Im Zugriffsmanagement werden den Identitäten Berechtigungen zugeordnet. Das kann auf der Grundlage von Rollen (rollenbasiert – RBAC), von Eigenschaften (attributbasiert – ABAC) oder von expliziten Rechtezuweisungen geschehen.

IAM-Stand heute

Unternehmen und Organisationen haben über Jahre hinweg IAM-Lösungen für ihre internen IT-Systeme aufgebaut. Darin verwalten sie die Identitäten der eigenen Mitarbeitenden und externer Benutzerinnen und Benutzer (z. B. Kunden oder Lieferanten) sowie deren Zugriffsrechte für ihre verschiedenen Applikationen. Die Informationen werden dabei selber erhoben und gepflegt. Existiert keine zentrale Benutzer- und Rechteverwaltung, ist dies oft mit grossem administrativen Aufwand und hohen Kosten verbunden. Denn so müssen die Benutzerdaten und -berechtigungen für jede Applikation einzeln gepflegt oder regelmässig repliziert werden. Das birgt neben dem erhöhten Fehlerpotenzial Sicherheitsrisiken und verursacht einen x-fachen Pflegeaufwand.

Die zunehmende Öffnung der Unternehmen und Organisationen sowie die Bereitstellung von Diensten im Internet lassen die vorhandenen Lösungen an Grenzen stossen. Immer mehr externe Benutzerinnen und Benutzer wollen Zugriff auf Daten oder Services, zum Teil nur einmalig oder gelegentlich. Die Anzahl der intern zu verwaltenden Identitäten wächst damit stark an. Bedenkt man, dass beim IAM die Registrations-, Mutations- und Deregistrationsprozesse der Hauptkostenfaktor sind, besteht Handlungsbedarf. Hier kann ein föderiertes Identitätsmanagement Abhilfe schaffen.

Föderiertes Identitätsmanagement

Beim föderierten Identitätsmanagement geht man davon aus, dass sich Subjekte und Ressourcen in unterschiedlichen administrativen Domänen befinden. Innerhalb einer Domäne gibt es dabei schriftliche Richtlinien zur Verwaltung von Identitäten, das heisst, man kann davon ausgehen, dass einheitliche und eindeutige Identifikatoren verwendet werden. Will nun ein Subjekt einer anderen Organisation, und damit aus einer anderen Domäne, auf Ressour-

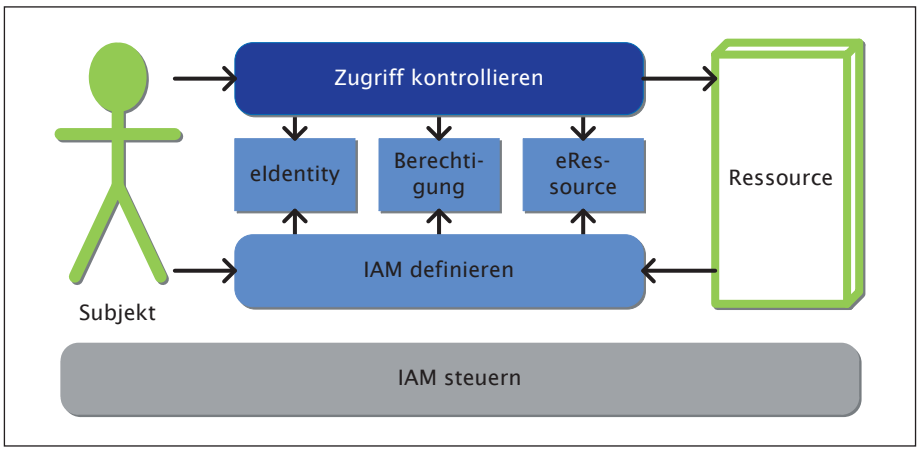

Abbildung 1: Bestandteile eines IAM

cen zugreifen, muss die Identität des Subjekts in der Zieldomäne bekannt gegeben werden. Dazu gibt es prinzipiell drei Lösungsansätze:

1. Direkte Replikation: Die betroffenen Domänen tauschen die Identitätsinformationen regelmässig aus.
2. Replikation zu Metadomäne: Die betroffenen Domänen tauschen die Identitätsinformationen mit einer vertrauenswürdigen dritten Partei aus.
3. Föderation: Die Zieldomäne vertraut der Authentifizierung der Heimorganisation des Subjekts.

Die Replikationslösung skaliert nur bei einer geringen Anzahl von kommunizierenden Domänen mit wenigen Benutzerinnen und Benutzern. Der fortlaufende Abgleich der Identitäten führt zu einem grossen administrativen Aufwand. Die zeitgerechte und vollständige Nachführung der externen Datenbestände stellt die Systemverantwortlichen vor Herausforderungen. Insbesondere das Nachführen des Austritts eines Subjekts aus der Heimorganisation geht vielfach in den replizierten Domänen verloren. Übrig bleibt ein verwaistes Benutzerkonto, das meist ein grosses Sicherheitsrisiko darstellt.

Der Metadomänenansatz hat gegenüber der direkten Replikationslösung den Vorteil, dass der Abgleich der Identitätsinformationen jeweils nur in eine Richtung erfolgen muss. Dadurch skaliert er auch besser bei einer grösseren Anzahl Domänen. Zudem kann der Abgleich einfacher standardisiert und dadurch besser automatisiert werden. Ein Nachteil besteht aber nach wie vor: Alle Beteiligten müssen ein hohes Mass an Vertrauen in die Metadomäne haben, und die Identitätsinformationen werden auch in diesem Modell repliziert und müssen in der Metadomäne sicher abgelegt werden.

Das föderierte Modell ist dagegen flexibler, erfordert aber Anpassungen der bestehenden Systeme. Der Vorteil einer Identity Federation liegt darin, dass Identitätsinformationen dort verbleiben, wo sie ihre prozessuale Hoheit haben, aber gleichzeitig für Services anderer Domänen benutzt werden können.

Grundbestandteile einer Identity Federation

Abbildung 2 zeigt das Schema eines föderierten Identitätsmanagements. 1) Das Subjekt möchte auf eine Ressource einer sogenannten Relying Party (RP) zugreifen, die einer anderen Domäne angehört. Das Subjekt wählt hierfür den Authentifizierungsdienst seiner Heimatdomäne und wird 2) von der Relying Party an den entsprechenden Identity Provider (IdP) weitergeleitet. 3) Dort authentifiziert sich das Subjekt, und 4) das Ergebnis wird in einer standardisierten Form gegenüber der anfragenden Stelle (Relying Party) bestätigt. Die Relying Party verifiziert die Antwort und gewährt dem Subjekt aufgrund der übermittelten Informationen Zugang zur Ressource oder weist dieses ab. Die Zugriffskontrolle (Feinautorisierung) erfolgt anschliessend lokal auf der Seite der Relying Party. Wenn notwendig, kann der Identity Provider weitere Informationen zum Subjekt, zum Beispiel die Zugehörigkeit zu einer Organisation oder die Funktion im Unternehmen, zusätzlich zur Authentifizierungsbestätigung mitliefern. Er agiert in diesem Fall als Attribut-Autorität (AA).

Damit die Identity Federation funktioniert, müssen die Systeme (RP und IdP/AA) einander vertrauen, eine Abstimmung der auszutauschenden Informationen vornehmen und die technischen Schnittstellen abgleichen. Das Standardprotokoll zum Austausch von Authentifizierungs- und Attributbestätigungen ist die Security Assertion Markup Language (SAML). Die in den Bestätigungen

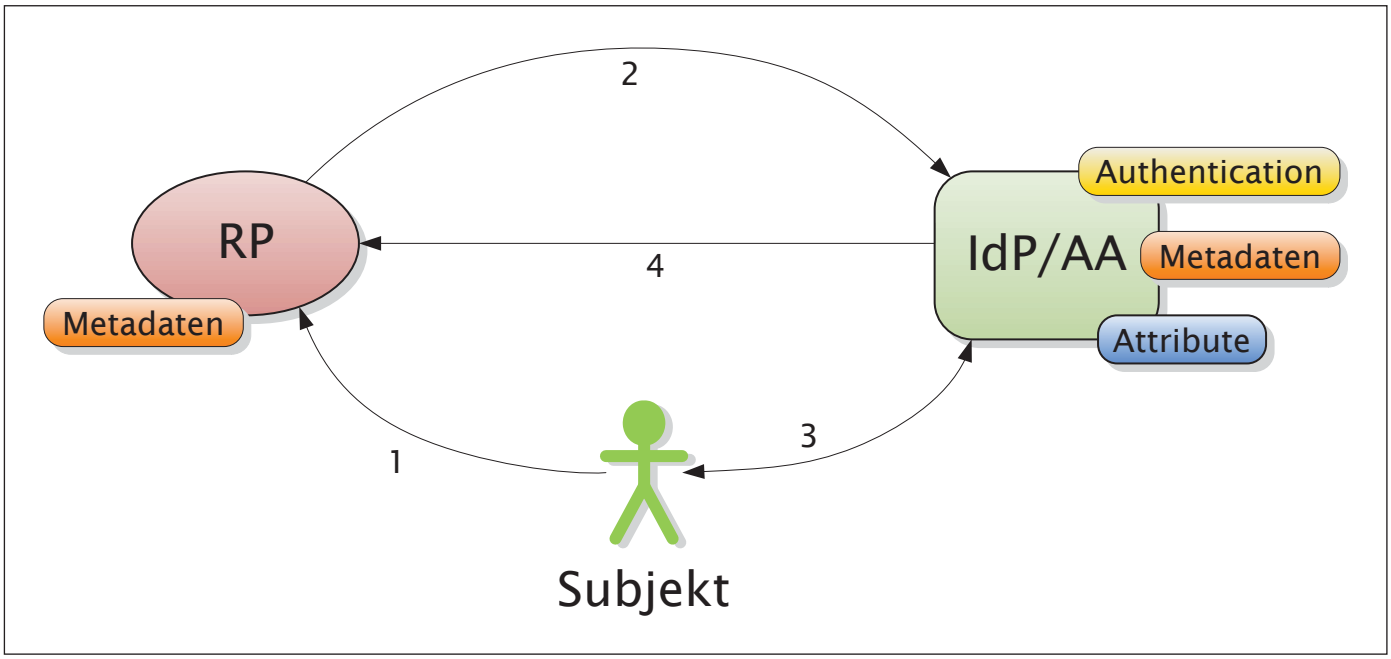

Abbildung 2: Schema einer Identity Federation

enthaltenen Informationen werden zuvor in Form von Metadaten ausgetauscht. Wichtig ist auch, dass die Semantik der ausgetauschten Informationen abgeglichen wird; alle Partner der Identity Federation sollten das gleiche Verständnis bei der Interpretation der Daten haben. Die Relying Party nutzt im föderierten IAM-Modell die IdP-Partner als autoritative Quelle für die Identitätsinformationen und delegiert die damit zusammenhängenden Managementaufgaben.

Identity-Federation-Modelle

Identity Federation gibt es je nach teilnehmenden Partnern in verschiedenen Ausprägungen. Stellt eine Relying Party Services für eine grosse Anzahl von Organisationen und Unternehmen bereit, spricht man vom RP-zentrierten Modell. Die Subjekte der Organisationen und Unternehmen authentisieren sich jeweils bei ihrem Heimat-IdP, und die zentrale Relying Party konsumiert die Authentifizierungs- und Attributbestätigungen der Informationslieferanten (IdP/AA). Der Vorteil dieses Ansatzes liegt darin, dass die Relying Party keinerlei Identitäten verwalten muss. Sie benutzt die Authentifizierungs- und Attributbestätigungen, um den Subjekten entsprechend Zugriff zu erteilen.

Ein Beispiel dieses Modells ist der Extranet-Zugang (RP) eines Dienstleisters für seine Kunden (IdP/AA). Damit wird den Kunden beispielsweise ermöglicht, die beim Dienstleister gekauften Produkte/Dienstleistungen online zu verwalten, ohne dass er (oder der Dienstleister) die einzelnen Benutzerkonten und deren Berechtigungen auf der Onlineplattform pflegen muss.

Konkret bietet dieser Ansatz folgende Vorteile:

- Auf der Plattform müssen keine spezifischen Benutzernamen und Passwörter bekannt sein. Dadurch entfällt die vorgängige Erfassung durch einen berechtigten Superuser des Kunden auf der Plattform, oder es geschieht automatisch bei Bedarf.
- Die Benutzerdaten und die Berechtigungen müssen nicht mehr auf der Onlineplattform gepflegt und aktualisiert werden. Die Daten werden während des Logins auf sichere Art und Weise übermittelt und bei Bedarf automatisch aktualisiert. Der Kunde steuert dabei, welche Daten bekannt gegeben werden.
- Die lokalen Berechtigungen werden aufgrund der übermittelten Benutzerdaten und vordefinierter Regeln definiert.
- Wenn ein Mitarbeiter die Firma des Kunden verlässt, muss das Benutzerkonto nicht mehr gelöscht werden. Sobald für einen Mitarbeiter ein Login in seiner Firma nicht mehr möglich ist, kann er sich auch auf der Onlineplattform nicht mehr anmelden.

Im umgekehrten Fall kann auch ein zentraler IdP/AA verwendet werden, um die Authentifizierung bei möglichst vielen Relying Parties zu gewährleisten. Ein Beispiel für das IdP/AA-zentrierte Modell ist der SuisseID IdP, der von einer Menge von Webshops und anderen Internetanwendungen verwendet wird. Dieses Modell lässt sich meist recht einfach innerhalb von bestehenden Organisationen umsetzen. Notwendig ist hierzu ebenfalls ein zentraler interner Identity Provider oder ein Direktzugriff auf einen Verzeichnisdienst, der dann von den verschiedenen Applikationen verwendet wird.

In der Praxis sind Identity-Federation-Implementierungen selten reine RP- oder IdP-zentrierte Modelle. Im gängigen Cross-Domain-Modell kann jede Organisation sowohl Identity Provider wie auch Relying Party sein. Dies ist ein häufiges Szenario, wenn ein IdP/AA-zentriertes Modell nicht umgesetzt werden kann. Alle Organisationen stellen auf der einen Seite die Identitäten ihrer Subjekte nach aussen zur Verfügung und betreiben auf der anderen Seite selbst Ressourcen, die sowohl von internen als auch von domänenexternen Subjekten verwendet werden können. Dieses Modell stösst an seine organisatorischen Grenzen, wenn der Verbund der Teilnehmer zu gross wird und die notwendigen Informationen bilateral ausgetauscht werden müssen. In diesem Fall sollten einzelne Dienste separiert, zentralisiert und von einem vertrauenswürdigen Betreiber unterhalten werden. Insbesondere ist es sinnvoll, in einem ersten Schritt die Metadaten der Relying Parties und der Identity Provider sowie die Auswahl der Authentifizierungsstellen zu zentralisieren.

Die Zukunft

Eine weitaus komplexere, aber auch nutzerfreundlichere Art stellt das sogenannte Hub-and-Spoke-Modell dar. Dabei hat ein Identity Hub eine erweiterte zentrale Rolle als Vermittler zwischen den Relying Parties und den IdP/AA-Anbietern. Die Kommunikation wird direkter, da die RP nur noch mit dem Hub kommunizieren und dieser die Anbindung der IdP/AA übernimmt. Er ermöglicht auch, dass Authentifizierungs- und Attributbestätigungen von unterschiedlichen IdP/AA zusammengetragen und konsolidiert werden können. Die neu entstehenden indirekten Vertrauensbeziehungen und der indirekte Informationsaustausch stellen den Hub-Betreiber vor juristische und organisatorische Herausforderungen. Die generischen Identity-und-Access-Management-Services von SuisseTrustIAM[2] basieren auf diesem Modell.

Unabhängig von der Art des eingesetzten Identity-Federation-Modells (auch Mischformen der oben genannten Modelle sind möglich) stellt die elektronische Zusammenarbeit über Organisationsgrenzen in jedem Fall eine Herausforderung an die Planung, die Vereinheitlichung der Prozesse und die Semantik der Informationen sowie an die technische Infrastruktur dar. Je grösser ein Organisationsverbund in einer Identity Federation ist, umso zwingender ist es, dass ein vertragliches Regelwerk die Richtlinien für die Beziehungen der einzelnen Parteien festlegt. Aus juristischer Sicht stellt dieses Modell des Informationsaustausches über Organisationsgrenzen hinweg noch eine recht grosse Hürde dar, die wohl erst durch die Gesetzesänderungen im Zusammenhang mit dem geplanten elektronischen staatlichen Identifikationsmittel (Revision ZertES) ausgeräumt werden wird.

Ausblick

Föderiertes IAM auf Basis einer Identity Federation bietet wirtschaftliche Vorteile, aber auch Vereinfachungen für die teilnehmenden Organisationen und Unternehmen. Die gemeinsame Nutzung von Ressourcen oder Identitätsinformationen führt vor allem langfristig zu einer Kostenersparnis und der Konsolidierung von Prozessen. Nicht zuletzt profitieren die Endbenutzerinnen und -benutzer davon, die eine digitale Identität für eine Vielzahl von Anwendungen benutzen können, statt für jede einen eigenen Benutzernamen plus Passwort zu pflegen.

Heute liegt die Verantwortung für das Zugriffsmanagement bei der Relying Party, die damit den Zugriff auf ihre Ressourcen selbst steuert. Mit der Einführung von Identity Federation ist es möglich, die Informationen für die Grobautorisierung für eine Ressource ebenfalls von einem gemeinsam genutzten, zentralen Dienst abzuholen. Dieser Zugangsservice würde der Relying Party eine Zugriffsentscheidung auf der Grundlage einer erfolgreichen Authentisierung und der Bestätigung von Attributen liefern. Speziell im E-Government-Umfeld, wo die Zugehörigkeit zu einer Gemeinde oder einer anderen Verwaltungsorganisation eine ausreichende Bedingung für den Zugang zu Applikationen darstellt, könnte dies einfach realisiert werden.

1 Siehe hierzu eCH-0107 http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0107
2 Siehe hierzu eCH-0167 http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0167