Sonderdruck
aus IT Spektrum 03/2026

Ausgabe 3/2026

IT Spektrum

Digitaler Wandel & Software-Architektur für Profis

Token Exchange als Katalysator der KI-Wertschöpfung

@nvd9612, pixabay

Sonderdruck aus IT Spektrum 03/2026

Token Exchange als Katalysator der KI-Wertschöpfung

Der KI-Einsatz zur Verknüpfung relevanter Informationen ist herausfordernd, wenn Daten über interne und externe Quellen verteilt liegen, verschiedene Identity Provider (IdP) und Authentifizierungsverfahren genutzt werden und es spezifische Sicherheitsvorgaben zu beachten gilt. Dem Variantenreichtum können IT-Architekten mit dem Token-Exchange-Lösungsansatz sicher und wirtschaftlich begegnen.

Das Aufmacherbild wurde per KI generiert.

Wettbewerbsfähigkeit und Datensicherheit dürfen sich niemals gegenseitig behindern. Unter dieser Prämisse ist es wichtig, KI-Agenten als eigene, digitale Identität im Rahmen eines stringenten Identitäts- und Zugriffsmanagements zu behandeln und gleichzeitig dafür zu sorgen, dass eine identitätszentrierte Steuerung nicht an den Eigenheiten einzelner Zugriffsziele scheitert.

Der „Token Exchange"-Mechanismus (Spezifikation RFC 8693 [https://datatracker.ietf.org/doc/html/rfc8693]) des Autorisierungs-Frameworks OAuth 2.0 [https://auth0.com/docs/authenticate/protocols/oauth] bietet hier ein wirksames Mittel, um die Schlagkraft KI-basierter Auswertungen ohne umfangreiche und in der Regel äußerst kostspielige Anpassungsaufwände für Unternehmen zu entfesseln.

Komplexität auf Unternehmensseite ist die Realität

Das Beispiel eines global agierenden Pharmakonzerns zeigt die Problematik: Hinter dem Vorhang eines solchen Konzernkonglomerats schlummern Abermillionen an Daten, die KI-gestützte Entscheidungsprozesse erheblich verbessern können. Interne Datenquellen sind dabei besonders relevant, weil ihre Qualität und Verlässlichkeit im Vergleich zu externen Informationen meist deutlich höher sind.

Die Realität ist jedoch von einer stark fragmentierten Systemlandschaft geprägt: von ERP-Systemen, Mail-Anwendungen, Fileservern, CRM oder Intranet über Collaboration-Plattformen wie SharePoint und Entwicklungsdatenbanken bis hin zu standort- oder bereichsspezifischen Eigenentwicklungen. Viele dieser Systeme werden unterschiedlich betrieben – On-premises, in der Cloud oder hybrid. Durch Merger-&-Acquisition-Strategien oder Partnerschaften steigt die Komplexität weiter.

Die Herausforderung bei der Suche nach relevanten und intern verborgenen Daten zur Beantwortung spezifischer Fragestellungen – à la „Wie ist der Stand der Entwicklung von Medikament xy? Wo liegen länderspezifische Risiken und Chancen? Welche Vorarbeiten wurden bereits geleistet? Welche Zertifizierungen liegen vor?" – wird umso größer. Moderne KI-Technologien, richtig angewendet und souverän abgesichert, können diese verstreuten Ressourcen innerhalb kürzester Zeit verknüpfen und Geschäftsprozesse entscheidend beschleunigen.

KI-Agenten als eigene Identität

Damit KI-Agenten sicher agieren können, benötigen sie eine klar definierte, nicht missbrauchbare Identität. Es reicht nicht, Agenten „barrierefreien" Zugang zu ermöglichen. Entscheidend sind die gezielte Steuerung der Datenabfrage und ein granulares Berechtigungsmanagement. Wie jeder interne Mitarbeitende dürfen auch KI-Agenten nur die Zugriffsmöglichkeiten erhalten, die sie für die jeweilige Aufgabe benötigen. Wer Hackern oder auch unberechtigten Anwendern im eigenen Ökosystem – im konkreten Fall eventuell einem chinesischen Partner – nicht Tür und Tor zu vertraulichen oder erfolgskritischen Daten öffnen möchte, benötigt eine identitätszentrierte Architektur, in der KI-Agenten in definierten Sicherheitszonen agieren.

Herausforderung 1: Authentifizierung von Non-Human Identities

Bei jeder KI-Abfrage über die verschiedenen Informationsquellen hinweg handelt es sich um Machine-to-Machine-Kommunikation. KI-Agenten fungieren als Non-Human Identities (NHI).

Zahlreiche aktuelle KI-Anwendungsszenarios zeigen hier Sicherheitslücken und mangelnde Transparenz. Viele NHI werden „irgendwo" manuell erzeugt und per Skript involviert – und ohne zentrales IAM-System (Identity & Access Management) verwaltet. Wenn heute KI-Tools wie ChatGPT, Perplexity, Claude oder Copilot in automatisierten Prozessen eingesetzt werden, herrscht im Hinblick auf zentrale Identitätssteuerung oder Sicherheitskontrolle in der Regel Fehlanzeige. Auf diese Weise entstehen und agieren zahlreiche Identitäten außerhalb des geschützten Rahmens. Unternehmen, die dies ändern möchten, dürfen dabei nicht vergessen, dass eine sichere Authentifizierung von NHI ganz eigene Ansprüche stellt. Denn ohne Benutzer aus Fleisch und Blut ist auch keine Multi-Faktor-Authentifizierung auf Basis biometrischer Merkmale möglich.

Anstelle der traditionellen Authentifizierung tritt der Umgang mit spezifischen Keys, die oftmals hart codiert – also direkt in den Quellcode eines Programms eingebettet – sind. Jede Änderung erfordert somit Anpassungen auf tiefster Ebene. Und nicht wenige Unternehmen haben bei Zertifikatsverwaltung und Secrets-Rotation massiv zu kämpfen, wenn die entsprechenden Keys ablaufen oder kompromittiert werden.

Ein Machine Identity Management (MIM) einzuführen oder das IAM um NHI-Prozesse zu erweitern, wird deshalb unverzichtbar. Für die NHI-Absicherung ist eine eindeutige Maschinenidentifikation durch Zertifikate, OAuth2-Client-Credentials oder SSH (Secure Shell Protocol)-Key-Verwaltung essenziell. Ebenso wichtig sind ein Lebenszyklus-Management, das automatisiert die Erstellung, Rotation und Löschung von Maschinenidentitäten steuert, sowie ein feingranulares Rechtemanagement, das Maschinenzugänge im Least-Privilege-Prinzip durchsetzt. Gleichzeitig sollte eine Zugriffsprotokollierung sicherstellen, dass auch maschinelle Interaktionen nachvollziehbar bleiben.

Herausforderung 2: Umgang mit vielfältigen IdP der potenziellen Quellsysteme

Wer Auswertungen über unterschiedliche Informationsquellen fahren will, muss der Anzahl und dem Variantenreichtum der IdP gerecht werden und in der Lage sein, mit einer Vielzahl interner und externer Identitätsquellen zu interagieren.

Dies fängt bei individuellen lokalen Verzeichnisdiensten oder Entra ID an und hört bei Google Identity bei Weitem nicht auf. In der Praxis existieren verschiedenste IdP parallel nebeneinander. Unterschiede in Protokollen (OAuth2, OpenID Connect, SAML – Security Assertion Markup Language usw.), Trust-Niveaus und Verwaltungskonzepten erschweren eine konsistente Autorisierung. Multi-IdP-Anforderungen durch Parallelnutzung mehrerer Systeme gehen mit komplexen Authentifizierungsflüssen auf Basis vielfältiger Tokenformate, Claims-Standards und Vertrauensanker einher.

Ein Federation-Layer, das ist eine Komponente in Datenmanagementsystemen, die es ermöglicht, Daten aus verschiedenen Quellen zu integrieren, oder ein entsprechend erweitertes IAM-System ermöglichen dynamisches IdP-Routing und bringen zusätzliche Flexibilität. Zugleich gilt es wie bereits angesprochen, auch für Non-Human Identities kontextsensitive Authentifizierung zu ermöglichen und zugrunde liegende Claim-Mappings und Trust-Policies so weit wie möglich zu standardisieren.

Token Exchange gewährleistet Sicherheit und Flexibilität bei minimalem Integrationsaufwand

Wer als Unternehmen KI-Agenten zu überschaubaren Kosten einen kontrollierbaren und gleichzeitig systemübergreifen Zugriff auf relevante Informationen in komplexen Umgebungen ermöglichen möchte, kommt an der Funktion des Token Exchange nicht vorbei. Der nach RFC 8693 spezifizierte Dienst innerhalb einer OAuth-/OIDC-Infrastruktur schafft selbst in komplexen Integrationsszenarien den Brückenschlag. Spezifische Token werden automatisiert in andere IdP-eigene und vertrauenswürdige Tokens umgewandelt. Dadurch wird höhere Zugriffskontrolle, Interoperabilität und Skalierbarkeit gewährleistet – auch in Multi-Cloud-Umgebungen. Ressourcenzugriffe lassen sich auf diese Weise ebenso granular wie dynamisch gestalten und gemäß Zero-Trust-Prinzip auf einzelne Zugriffe beschränken.

Überblick Funktionsweise

Beim IdP-übergreifenden Handling von Berechtigungstoken übernimmt Token Exchange die Rolle des „Dolmetschers". Eingehende Token, die bereits eine spezifische Identität und Vertrauensbeziehung belegen, werden entgegengenommen, geprüft und in neue Token umgewandelt, die dann den Zugriff auf weitere konkrete Ressourcen erlauben (siehe Abb. 1) und gegebenenfalls auch gleichzeitig für andere Sicherheitsdomänen (beispielsweise mit anderen Signaturschlüsseln) oder auch mit angepassten Claims – etwa geänderter Subject-Identität, Audience oder Scopes – gelten.

Zur Präzisierung dient das genannte Beispiel des Pharmaunternehmens, bei dem es fünf verschiedene IdP zu beachten gilt, darunter je einer für die Microsoft-Welt, das SAP-System, das Partnerportal und das IAM mit MFA (Multi-Faktor-Authentifizierung). Zudem verwendet ein Joint Venture des Konzerns, das für den Produktionsstandort in China gegründet wurde, ein separates Identitäts- und Rechtemanagement mit eigenem IdP.

Wenn KI-Tools für Auswertungen alle unternehmensweit verfügbaren Daten berücksichtigen sollen, kann Token Exchange nicht nur den Ressourcenzugriff auf einfache Weise ermöglichen. Zugleich lässt sich auch die Autorisierung für den Ressourcenzugriff jedes Mal überprüfen und somit sicherer gestalten. Policy-Enforcement-Komponenten in einzelnen Sicherheitszonen validieren ausschließlich die Token, die für ihre Zone bestimmt sind, basierend auf den jeweils passenden Schlüsseln. Damit ist eine strikte Trennung von Sicherheitsdomänen umsetzbar, während gleichzeitig ein kontrollierter Austausch von Vertrauensinformationen möglich bleibt.

Sobald ein in der Microsoft-Welt etabliertes KI-Tool (Non-Human Identity) wie Copilot auch auf das interne SAP-System des Unternehmens zugreifen möchte, entfaltet das Zusammenspiel von WAAP-Lösung (Web Application and API Protection) und Token-Exchange-Server Wirkung. Die vorgelagerte WAAP-Komponente leitet

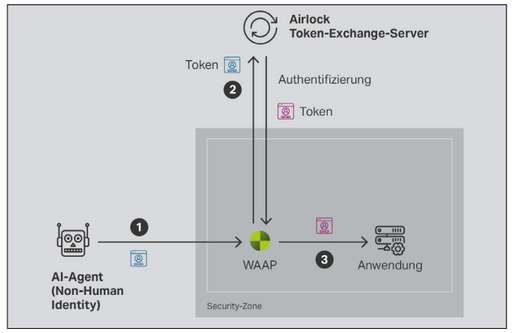

Abb. 1: Beispielhafte Verarbeitung des Tokens beim Zugriff eines KI-Agenten auf ein Backend-System

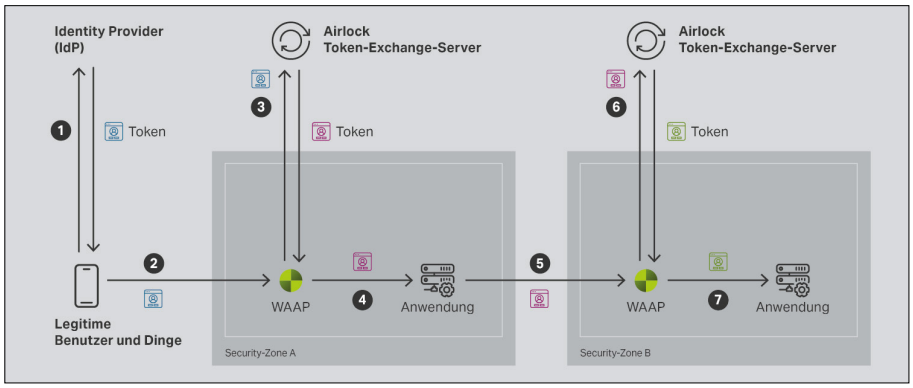

Abb. 2: Brückenschlag zwischen unterschiedlichen Sicherheitszonen

Sicherheitszonen	In diesem Szenario in Abb. 2 sind unterschiedliche Sicherheitszonen dargestellt (Security-Zone A, Security-Zone B). In diesen sind jeweils eigene Sicherheitstoken erforderlich, die nur in dieser Zone gelten. Die Token werden vom Token-Exchange-Server (Standalone OAuth AS) ausgegeben.
Token-Exchange-Server	Der Token-Exchange-Server empfängt Anfragen in Security-Zone A mit blauen Tokens als Subject Token. Der Token-Exchange-Server gibt je nach Zielgruppe oder Ressourceninformationen rote Tokens aus.
PEP	Die Policy Enforcement Points (PEP) in diesen Zonen validieren die Token anhand des Schlüsselmaterials entweder aus dem FE OAuth AS oder dem Token-Server (Security-Zone A und Security-Zone B). Jeder PEP validiert nur die Token seiner eigenen Sicherheitszone.
Client	Der Autorisierungsserver der Security-Zone A akzeptiert nur Endbenutzer/NHI-Clients, die Sicherheitstoken anfordern. Typische Token-Anforderungen in dieser Zone verwenden den Autorisierungscode-Flow. Der Token-Austauschserver (Standalone OAuth AS) akzeptiert nur Server aus Security-Zone A als Clients. Auf solchen Servern können ausgetauschte Token abgerufen werden.

Tabelle 1: Erläuterung zur Token-Verarbeitung über unterschiedliche Sicherheitszonen hinweg

die Anfrage automatisiert zum Token-Exchange-Server um, der das entsprechende Nutzer-Token prüft und nach Authentifizierung durch ein Zugriffs-Token für SAP ersetzt (siehe Abb. 2, Tabelle 1). Einem systemübergreifenden Agieren von KI-Agenten steht somit nichts mehr im Wege. Architektonisch kann der Token-Exchange-Dienst separat betrieben werden, um die Sicherheitsdomänen klar voneinander zu trennen, oder integriert mit einem bestehenden Autorisierungsserver, um den Installationsaufwand zu reduzieren. Eine vollständig segregierte Variante, bei der jede Domäne ihren eigenen Token-Exchange-Dienst betreibt, erhöht die Sicherheit und die Kontrolle über Schlüsselmaterial und berechtigte Clients, geht aber mit höherem Betriebs- und Konfigurationsaufwand einher.

Fazit: Token Exchange schafft Einklang aus Sicherheit, Flexibilität und Wirtschaftlichkeit

Die Anzahl der verschiedenen IdP wird sich in naher Zukunft kaum reduzieren. Gleichzeitig kommt über kurz oder lang kein Unternehmen am Thema KI – und damit auch an Fragestellungen zum idealen Umgang mit Non-Human Identities – vorbei. Zugriffsrechte für einzelne IdP lassen sich bereits heute elegant verwalten. In der Gesamtheit wird es jedoch schwierig und der ganzheitliche Blick scheitert an den spezifischen Silostrukturen mit jeweils eigenen Token, die die Machine-to-Machine-Kommunikation behindern.

Genau an dieser Stelle spielt der Token-Exchange-Server seine Stärken aus. Dieser verheiratet die unterschiedlichen Prozedere, ohne dabei die Kontrolle über das Zugriffsmanagement und die Rechteverwaltung zu verlieren. Im Gegensatz zur Alternativoption, alle gewünschten Systeme auf einen einzigen IdP wie beispielsweise Entra ID umzustellen, ist dieser Ansatz nicht nur günstiger, sondern darüber hinaus auch in viel kürzerer Zeit realisierbar. Zudem können neue Zielsysteme im Unternehmen, beispielsweise nach Akquisitionen, jederzeit flexibel angebunden werden. Einzelne Applikationen müssen nicht verändert werden.

Für Organisationen, die vor der Herausforderung stehen, Non-Human Identities in Form von KI-Werkzeugen und komplexe Informationslandschaften in den eigenen Reihen in ein sicheres Zusammenspiel zu bringen, liefert das Konzept von Token Exchange derzeit gewiss einen spannenden Ansatz.

Die Autoren

Detlev Altendorf
detlev.altendorf@airlock.com
ist seit über 15 jahren im IT-Security-Vertrieb engagiert. Die Verschlüsselung von Daten auf mobilen Geräten, eine sichere Datenübertragung, das Management von Identitäten und der einfache (SSO) und trotzdem sichere (2FA) Zugriff auf Web-Services standen in dieser Zeit immer im Fokus. Für Airlock zeichnet er seit 2024 als Account und Partner Manager verantwortlich.

Stefan Braun
sbraun@airlock.com
stieß 2024 zu Airlock. Zuvor war der Senior Security Consultant bei A10 Networks tätig. Weitere berufliche Stationen waren bei Radware und Allot Communications, wo er in der Rolle des Professional Service Engineers agierte. Seine Karriere begann der gelernte IT-Systemelektroniker beim Bundesministerium für Wirtschaft und Technologie in Bonn.