

MEDIENMITTEILUNG

Zürich, 11. Februar 2026

Token Exchange: Identitäten sicher über Domänengrenzen hinweg autorisieren

Einsatz von KI-Agenten, APIs und Microservices erfordert sichere Authentisierung von Identitäten über mehrere Sicherheits- und Vertrauensdomänen hinweg – eine Herausforderung, die mit Token Exchange beherrschbar wird

Der KI-Funke lodert immer stärker: Zunehmend mehr Unternehmen träumen von hauseigenen Chatbots, die den Beschäftigten Antworten aus dem gesamten Unternehmensnetz zusammentragen, und KI-Agenten, die Workflows und Geschäftsprozesse automatisieren. Doch an der Grenze einer Identitätsdomäne – etwa der Microsoft-365-Welt mit Entra ID – heisst es für Anwender und KI-Bots schnell: «Ende der Ausbaustrecke», beispielsweise beim Zugriff auf SAP-Anwendungen. In dem Zusammenhang verzeichnet der Sicherheitsanbieter Airlock derzeit eine steigende Nachfrage nach Lösungen, die dem KI-Einsatz trotz Parallelbetrieb von Identitätsdomänen mit separaten Identity Providern (IdP) sicher und kosteneffektiv Rechnung tragen. Um Unternehmen hier Orientierung zu bieten, rückt der Spezialist für Identitätsmanagement das Konzept des «Token Exchange» in einem aktuellen Whitepaper in den Fokus.

Mit der bereits 2024 ins Airlock-Produktportfolio integrierten «Token Exchange»-Funktionalität (Spezifikation RFC 8693) des Autorisierungs-Frameworks OAuth 2.0 spielt es keine Rolle, ob entscheidungsrelevante Informationen über vielfältige interne und externe Quellen verteilt liegen und wie viele Identity Provider (IdP), Authentifizierungsverfahren und spezifische Sicherheitsvorgaben es im Zuge dessen zu berücksichtigen gilt. Die Fähigkeit zum Token Exchange im Rahmen einer zentralen Identitätssteuerung eröffnet Organisationen im wahrsten Sinne des Wortes «grenzenlose» Freiheit zur Entfesselung des KI-Potenzials. Der Vorteil: Einzelne Systeme der Identitätsverwaltung müssen nicht individuell aufwendig angepasst werden. Der Brückenschlag via Token Exchange ist mit deutlich geringeren Kosten verbunden und die Einsatzmöglichkeit bei Weitem nicht nur auf Non-Human-Identities beschränkt. Vielmehr wird Token Exchange zur entscheidenden Schlüsselzutat einer identitätsbasierten Absicherung komplexer IT-Landschaften.

«Token Exchange hilft Unternehmen, unterschiedliche Identity Provider und Tokenformate sicher zusammenzubringen, ohne tief in bestehende Anwendungen eingreifen zu müssen. Das reduziert Aufwand sowie Kosten und erhöht gleichzeitig die Flexibilität», so Stefan Braun, Senior Security Consultant bei Airlock.

IdP-übergreifendes Handling von Berechtigungstoken

Beim IdP-übergreifendem 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 und gegebenenfalls auch für andere

MEDIENMITTEILUNG

Sicherheitsdomänen (beispielsweise mit anderen Signaturschlüsseln) oder auch mit angepassten Claims – etwa geänderter Subject-Identität, Audience oder Scopes – gelten. Ressourcenzugriffe lassen sich auf diese Weise ebenso granular wie dynamisch gestalten und gemäss Zero-Trust-Prinzip auf einzelne Zugriffe beschränken. Inkonsistente Berechtigungen durch stockende Kommunikation aufgrund der Protokollvielfalt sowie mangelnde Nachvollziehbarkeit sind damit passé.

Herausforderung in Kubernetes-Umgebungen allgegenwärtig

Handlungsbedarf zeigt sich nicht zuletzt vor dem Hintergrund der wachsenden Bedeutung von Microservices und damit der Container-Orchestrierungsplattform Kubernetes. Neben einer domänenübergreifenden Kommunikation zählt der Schutz vor Angriffen und Missbrauch mehr denn je. Hier schafft identitätszentrierte, dezentrale Kontrolle – bei der der Token-Exchange-Server von Airlock bei der Autorisierung die Vermittlungsrolle übernimmt – Abhilfe. Das vorgeschaltete, leichtgewichtige Microgateway gewährleistet die Introspektion von OIDC- oder JWT-Token (OpenID Connect, JSON Web Token) und prüft, ob ein gültiges Token vorhanden ist, bevor es den Zugriff auf den zugehörigen Microservice gestattet.

Token Exchange in der Praxis

Bei der Schweizerische Bundesbahnen AG gehört dies bereits seit 2024 zum Tagesgeschäft. Im konkreten Einsatzszenario sorgt Token Exchange dafür, dass sich mehrere hundert Service-Anbieter bei gezielter Segmentierung sicher auf einer Plattform integrieren lassen. So laufen Frontend- und Backend-Server beispielsweise in unterschiedlichen Sicherheitszonen, die über jeweils eigene Zugriffstoken verfügen. Der Frontend-Server kann nicht einfach das bestehende Token weiterleiten, sondern muss dieses beim Autorisierungsserver in ein neues Token umtauschen. Auf diese Weise lässt sich effektiv verhindern, dass Angreifer von einem kompromittierten System auf weitere Server zugreifen. Der Token Exchange ist dabei vollständig in die vorgelagerte IAM-Lösung von Airlock integriert. Der Vorteil der standardisierten, zentralen Authentifizierungsplattform liegt nicht nur in der ausgeprägten Skalierbarkeit, sondern insbesondere auch in der hohen Verfügbarkeit und Systemsicherheit, die selbst in Multi-Cloud-Umgebungen jederzeit garantiert sind.

Weiterführende Informationen im Whitepaper

Wie Security-Verantwortliche Identitäten in modernen IT-Landschaften – als Mix von Cloud-, On-Premises- und Kubernetes-Umgebungen – über Domänengrenzen hinweg zuverlässig autorisieren können, ohne dass es zu Einbussen im Hinblick auf Agilität und Benutzerfreundlichkeit kommt, zeigt das neue Whitepaper von Airlock im Detail:

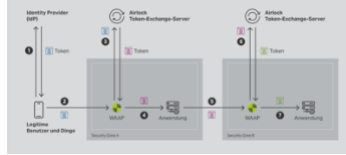
<https://www.airlock.com/sprechen-sie-token>

MEDIENMITTEILUNG

Bildmaterial



Stefan Braun, Senior Security Consultant bei Airlock Nutzerzugriff auf einen Frontend-Service



Weitere Informationen:

Airlock

Ergon Informatik AG
Gernot Bekk-Huber
gernot.bekk-huber@ergon.ch
+41 78 955 35 60
Merkurstrasse 43
CH-8032 Zürich

Press'n'Relations GmbH

Rebecca Horn
rh@press-n-relations.de
+49 731 146 156-75
Magirus-Deutz-Str. 14
D-89077 Ulm

Über Airlock

Der Airlock Secure Access Hub vereint seit 20 Jahren die kritischen IT-Sicherheitsthemen der Filterung und Authentisierung zu einem gut abgestimmten Gesamtpaket, das Massstäbe in Sachen Bedienbarkeit und Services setzt. Der Secure Access Hub deckt alle wichtigen Funktionen der modernen Applikationssicherheit ab: von einer durch Fachjournalisten ausgezeichneten Web Application and API Protection (WAAP), über ein Microgateway für Sicherheit in Kubernetes-Umgebungen, hin zu einem Identitäts- und Zugriffsmanagement (IAM) mit integrierter starker Authentifizierung. Die IT-Sicherheitslösung Airlock schützt mehr als 30 Millionen aktive, digitale Identitäten und 30.000 Back-Ends von über 600 Kunden auf der ganzen Welt. Weitere Informationen unter <https://www.airlock.com>.

Airlock ist eine Security Innovation des Schweizer Softwareunternehmens Ergon Informatik AG. Das Unternehmen wurde 1984 gegründet, zählt rund 450 Mitarbeiter und wurde wiederholt als einer der beliebtesten Arbeitgeber der Schweiz ausgezeichnet.