AIRLOCK®
SECURE ACCESS HUB

Zero Trust und Airlock IAM

Wie die Schweizerische Bundesbahnen AG (SBB) über 260 Service-Anbieter auf einer Plattform integriert.

Bei Airlock arbeite ich mit echten Spezialisten zusammen, die mit ihrem Service immer wieder begeistern.

Michael Gerber, Senior Systemarchitekt bei der SBB

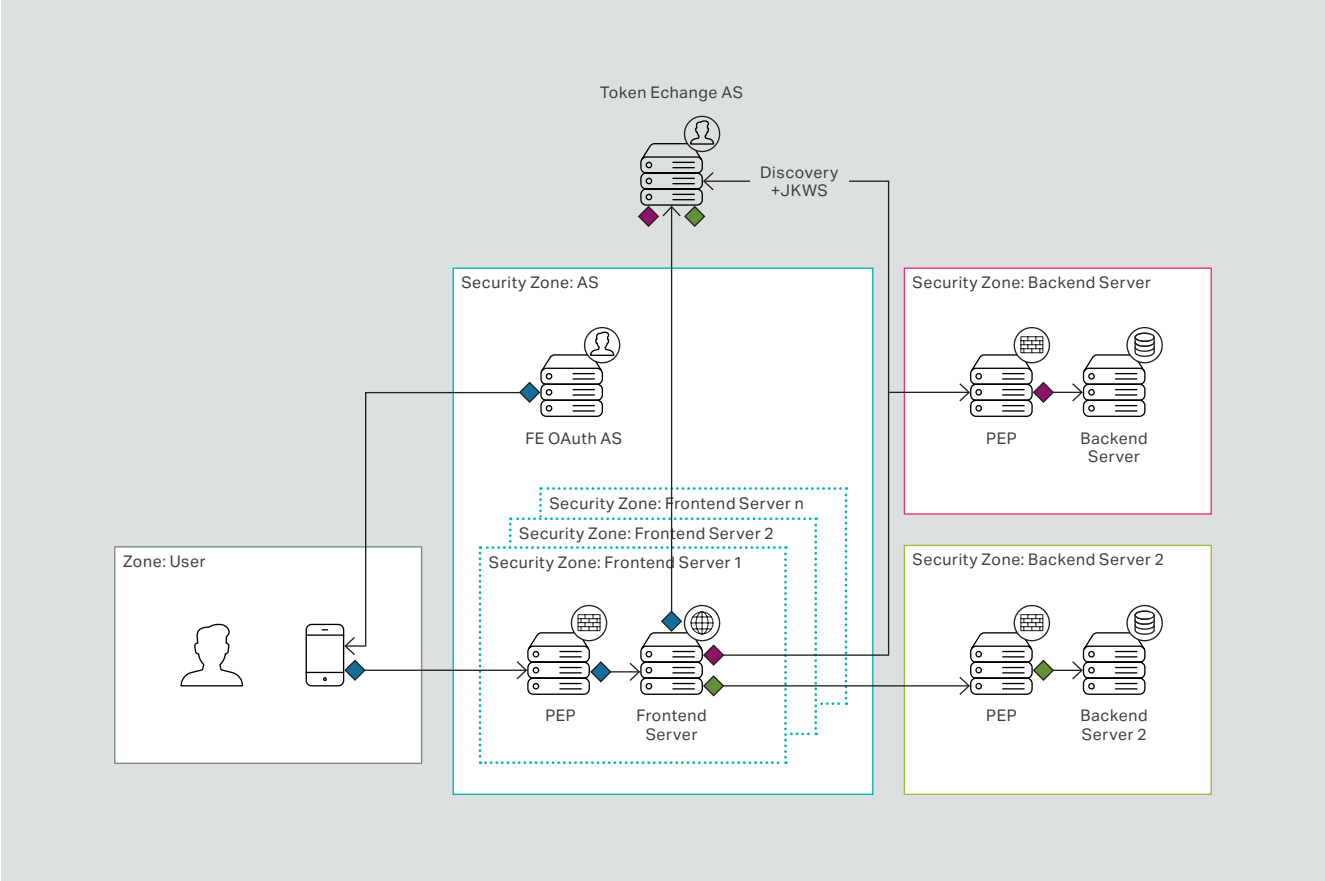
Sichere Verbindungen schaffen – das macht die Schweizerischen Bundesbahnen AG (nachfolgend SBB) seit über 200 Jahren. Beim Schienenverkehr. Und heute auch beim Datenverkehr. Denn wenn Kunden über eine zentrale Plattform Zugtickets kaufen, Wellness-Eintritte buchen und Sharing-Angebote nutzen, dann braucht es hierfür eine IT-Technologie, die vor allem eines garantiert: Sichere Verbindungen.

Der öffentliche Verkehr ist in der Schweiz ein hohes Gut und gehört punkto Qualität zu den weltweiten Spitzreitern. Ein wesentlicher Grund für diesen Erfolg: Kundenzentrierte Angebote, die immer wieder mit innovativen Leistungen überzeugen. So verwundert es nicht, dass die SBB zu den digitalen Vorreitern gehört, die heute nicht nur 420 Millionen Personen zwischen verschiedenen Städten transportieren, sondern auch Abermillionen von Daten mit anderen Anbietern austauschen – mit Leistungserbringen des öffentlichen Verkehrs, mit Tourismus-Organisationen, mit Sharing-Plattformen für die Auto- und Fahrrad-Miete.

Ein durchgängiges digitales Ökosystem und eine Single-Stop-Lösung

Was mit dem Datenaustausch erreicht werden soll? Ein integriertes Mobilitätangebot, das den Kunden «Ein Ticket für alles» zur Verfügung stellt. Der Vorteil für die Reisenden: Sie profitieren von einer Single-Stop-Lösung und einem durchgängigen digitalen Ökosystem – egal, ob sie den örtlichen Bus nehmen oder einen Tag auf der Skipiste geniessen möchten.

Doch so attraktiv «Ein Ticket für alles» auch klingt – technisch ist die Single-Stop-Lösung eine echte Herausforderung. Dabei steht vor allem die IT-



OAuth 2.0 nutzt Zugriffstokens, die kontextabhängig und rollenspezifisch ausgeben werden, und hat sich als massgeblicher Standard für Online-Autorisierungen durchgesetzt.

Security im Mittelpunkt. So müssen verschiedene Vertriebsorganisationen mit ihren eigenen Shop-Systemen und einer heterogenen Applikationslandschaft zuverlässig gemanagt werden – beim Schutz vor Missbrauch, beim Umgang mit sensiblen Kundendaten und bei finanziellen Transaktionen. Deshalb setzt die SBB auf zwei Konzepte, die heute dem State of Art entsprechen: auf Zero Trust und Token Exchange. Und natürlich auf das Identity and Access Management (IAM) von Airlock.

Zero Trust und Token Exchange
Zero Trust ist eine innovative Sicherheitsphilosophie, die auf einem zentralen Prinzip basiert: Benutzern, Geräten oder Anwendungen im Netzwerk wird automatisch misstraut. Daher müssen alle Zugriffe permanent authentifiziert und autorisiert werden, um auf sensible Ressourcen zugreifen zu können. So stellt das Konzept sicher, dass die Identität und Berechtigung der User ständig überprüft werden, um Sicherheitsrisiken zu minimieren.

Token Exchange ist ein technisches Verfahren, das den sicheren Austausch von Zugriffstoken zwischen verschiedenen Vertrauensbereichen ermöglicht. Diese Token dienen dazu, die Identität und Autorisierung eines Benutzers zu überprüfen, ohne die eigentlichen Anmeldeinformationen preiszugeben. Token Exchange erleichtert somit die Integration von Anwendungen zwischen verschiedenen Organisationen, ohne die Sicherheit zu gefährden.

OAuth 2.0 Token Exchange: Mehrfache Sicherheit dank gezielter Segmentierungen
So kann ein Frontend-Server beispielsweise einen Backend-Server kontaktieren, der in einer anderen Sicherheitszone läuft. Falls jede Zone über eigene Zugriffstokens verfügt, kann der Frontend-Server nicht einfach das bestehende Token weiterleiten, sondern muss diesen beim Autorisierungsserver in ein neues Token umtauschen. Mit dieser Segmentierung kann ein Angreifer beim OAuth 2.0 Token Exchange daran gehindert werden, von einem kompromittierten System auf weitere Server zuzugreifen.

Der erste Benefit dieser Lösung: Natürlich eine optimale IT-Sicherheit, die auch den neuesten regulatorischen Anforderungen entspricht. Und der zweite Benefit? Die SBB hat sich für das vorgelagerte IAM von Airlock mit integriertem Token Exchange entschieden – und damit für eine standardisierte Lösung, die sich schnell skalieren lässt und als zentrale Authentifizierungsplattform dient.

Unkomplizierte Sicherheit: Airlock IAM
Was die Airlock-Lösung besonders auszeichnet: Ihre hohe Verfügbarkeit und Systemsicherheit, die auch in Multi-Cloud-Umgebungen garantiert ist. Dazu Michael Gerber, der verantwortliche IT-Architekt bei der SBB: «Als Schweizer Qualitätsanbieter ist Airlock ein bewährter Partner unseres Unternehmens. So passt das Airlock IAM perfekt in unsere IT-Landschaft und gerade die unkomplizierte Integration hat uns überzeugt – sowohl bei der Anwendung über mehrere Instanzen als auch beim schnellen Deployment.» Zudem unterstreicht Michael Gerber einen weiteren entscheidenden Punkt: «Bei Airlock arbeite ich mit echten Spezialisten zusammen, die mit ihrem Service immer wieder begeistern.» So ist auch beim Support eine sichere Verbindung garantiert – mit schnellen Reaktionszeiten, fundierten Lösungen und einer zuverlässigen Unterstützung im täglichen Betrieb.

«Als Schweizer Qualitätsanbieter ist Airlock ein bewährter Partner unseres Unternehmens. So passt das Airlock IAM perfekt in unsere IT-Landschaft und gerade die unkomplizierte Integration hat uns überzeugt – sowohl bei der Anwendung über mehrere Instanzen als auch beim schnellen Deployment.»

Michael Gerber,
Senior Systemarchitekt bei der SBB

Über die SBB – Schweizerische Bundesbahnen AG
Das Unternehmen «Schweizerische Bundesbahnen SBB» ist eine spezialgesetzliche Aktiengesellschaft mit Sitz in Bern. Zu ihren Service-public-Leistungen gehören der Personenverkehr und die Schieneninfrastruktur. Sie bringt täglich über 1,16 Millionen Reisende und 185 000 Tonnen Güter ans Ziel.
Mehr als 33 000 Mitarbeitende setzen sich mit Leidenschaft für ihre Kund:innen ein, damit diese sicher, pünktlich und klimafreundlich ankommen.

Über Airlock – Security Innovation by Ergon Informatik AG
Der Airlock Secure Access Hub vereint die wichtigen 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 IT-Sicherheit in diesem Bereich ab: von einer durch Fachjournalisten ausgezeichneten Web Application Firewall (WAF), über ein Customer Identitäts- und Zugriffsmanagement (cIAM), dem Schweizer Banken vertrauen, hin zu einer API-Sicherheit, die neueste Anforderungen stemmt. Die IT-Sicherheitslösung Airlock schützt mehr als 20 Millionen aktive, digitale Identitäten und 30.000 Back-Ends von über 550 Kunden auf der ganzen Welt. Weitere Informationen unter www.airlock.com. Airlock ist eine Security Innovation des Schweizer Softwareunternehmens Ergon Informatik AG.

Die 1984 gegründete Ergon Informatik AG ist führend in der Herstellung von individuellen Softwarelösungen und Softwareprodukten. Die Basis für den Erfolg sind 300 hochqualifizierte IT-Spezialisten, die dank herausragendem Fachwissen neue Technologietrends schnell antizipieren und mit innovativen Lösungen entscheidende Wettbewerbsvorteile sicherstellen. Ergon Informatik realisiert hauptsächlich Grossprojekte im Bereich B2B.

Ergon Informatik AG
Merkurstrasse 43
CH-8032 Zürich
+41 44 268 89 00
info@airlock.com

www.airlock.com

ergon