

# Die Puzzleteile moderner Authentifizierung



Bauanleitung fürs cIAM



# Inhaltsverzeichnis

<b>Einleitung</b>	<b>3</b>
<b>1. Die Herausforderungen der Authentifizierung im Blick</b>	<b>4</b>
1.1 Non-Human Identities (NHI)	4
1.2 Wildwuchs der Identity Provider (IdP)	5
1.3 Device- und Kanalvielfalt	6
1.4 Kreativität der Angreifer	7
1.5 KI-Einsatz	8
1.6 Quantencomputing	9
1.7 Wettbewerbsfaktor Benutzerfreundlichkeit	10
<b>2. Relevante Puzzleteile im Zuge steigender Anforderungen</b>	<b>12</b>
2.1 Passwortlose Authentifizierung	13
2.1.1 FIDO2 als Allheilmittel?	13
2.2 Risikobasierte Authentifizierung	14
2.3 Continuous Adaptive Trust	15
2.4 SSI-Enablement	16
2.5 Post-Quanten-Kryptografie	17
<b>3. Best Practices: Die Bauanleitung für das Puzzle moderner Authentifizierung</b>	<b>18</b>
Unterstützung offener Standards	18
Flexible Flows	19
Effiziente Migration von Authentifizierungsmitteln	20
Unterstützung von Token Exchange	21
Integration von SSI	21
Zusammenarbeit mit WAAP-Systemen	22
Identity Federation und hybride Landschaften	23
Nähe zum Kunden und digitale Souveränität	24
<b>4. Airlock: Puzzlen mit Methode</b>	<b>25</b>
Aufbau und Struktur der Sicherheitsarchitektur	25
<b>5. Fazit</b>	<b>27</b>
<b>Glossar und Abkürzungen</b>	<b>28</b>
<b>Weiterführende Ressourcen</b>	<b>30</b>

# Einleitung

**Digitale Identitäten stehen im Zentrum nahezu aller modernen Geschäftsmodelle. Ihre sichere und effiziente Verwaltung entwickelt sich zunehmend zur Herausforderung für Unternehmen und öffentliche Einrichtungen. Wer Nutzer zuverlässig authentifizieren will, muss sensible Informationen schützen und gleichzeitig eine reibungslose Nutzererfahrung ermöglichen. Im Customer Identity and Access Management (CIAM) spielen moderne Authentifizierungsverfahren deshalb eine Schlüsselrolle: Sie helfen, Sicherheitsrisiken zu minimieren und das Nutzererlebnis spürbar zu verbessern.**

Dieses Whitepaper richtet sich an Verantwortliche für Identitäts- und Zugriffsmanagement in mittleren bis grossen Unternehmen. Die folgenden Seiten liefern praxisnahe Einblicke, technische Lösungsansätze und konkrete Handlungsempfehlungen, die helfen, die aktuellen Herausforderungen moderner Authentifizierung erfolgreich zu bewältigen.

Letztlich verhält es sich beim Identitätsmanagement nicht anders als bei einem Puzzle. Es gilt zunächst, eine klare Vorstellung vom Gesamtbild der Herausforderungen (Kapitel 1) zu gewinnen und zu verstehen, was die Aufgabe jedes einzelnen Puzzleteils ist (Kapitel 2). Mit der richtigen Herangehensweise (Kapitel 3) lässt schliesslich sich jedes noch so komplexe Puzzle erfolgreich zusammensetzen. Die umfassende Funktionsvielfalt von Airlock, das Fundament offener Schnittstellen sowie das Commitment zu künftigen Standards (Kapitel 4) können massgeblich dazu beitragen, Unternehmen schnell und erfolgreich ans Ziel zu bringen.

# 1. Die Herausforderungen der Authentifizierung im Blick

Authentifizierung wird komplexer – egal ob im Hinblick auf Security, Benutzerfreundlichkeit oder die Berücksichtigung neuer Technologien. Welche Trends sind dabei wegweisend? Im Folgenden wird ein Blick auf die wichtigsten Herausforderungen geworfen, die den Alltag der Verantwortlichen für Identitäts- und Zugriffsmanagement bereits heute beeinflussen und künftig weiter an Bedeutung gewinnen werden. Die Grenzen zwischen den einzelnen Themen sind oftmals fließend.

## 1.1 Non-Human Identities (NHI)

Automatisierung und Digitalisierung haben die Zahl digitaler Identitäten explodieren lassen. In modernen IT-Landschaften sind Maschinenkonten längst keine Randerscheinung mehr. Einschlägige Studien<sup>1</sup> gehen mittlerweile davon aus, dass das Verhältnis von menschlichen Identitäten und Non-Human Identities (NHI) bei 1:50 liegt, Tendenz steigend. Dabei ist es ganz egal, ob API, Microservice, IoT-Gerät, Container oder RPA-Bot (Robotic Process Automation) – sie alle agieren in der Regel als eigene, oft hochprivilegierte digitale Identität und benötigen ein ebenso stringentes Identitäts- und Zugriffsmanagement wie menschliche Nutzer. Ein offensichtliches Problem ist dabei nicht zuletzt die mangelnde Transparenz. Derzeit werden viele NHI noch «irgendwo» manuell erzeugt und per Skript eingebunden – ohne ein zentrales IAM-System. Somit gestaltet sich die sichere Authentifizierung schwierig. 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 Token, Zertifikaten oder sonstigen 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 Token oder API-Keys ablaufen oder kompromittiert werden.

**«KI-Agenten, die sich als menschliche Benutzer ausgeben und in Systeme einloggen, sind auf dem Vormarsch und müssen abgesichert werden. Die Anforderung an sich ist nicht neu. Beispielsweise gibt es schon lange Fintech-Drittanbieter-Apps, bei denen ein Bot im Kundennamen via API in Banksystemen auf die entsprechenden Daten zugreift. Hier zählen im Zuge von PSD 2 (Payment Service Directive 2) einschlägige Berechtigungshinweise. Mit dem Erstarken der künstlichen Intelligenz (KI) nimmt das Thema NHI inzwischen jedoch ganz andere Dimensionen an.»**

<sup>1</sup> [The Ultimate Guide To Non-Human Identities](#)



## Anforderung

Vor diesem Hintergrund kommt es umso mehr darauf an, ein Machine Identity Management (MIM) einzuführen und/oder das IAM um NHI-Prozesse bzw. Token Exchange Server zu erweitern. Für die NHI-Absicherung ist eine eindeutige Maschinenidentifikation durch Zertifikate, OAuth2-Client-Credentials oder SSH (Secure Shell Protocol)-Key-Verwaltung essenziell. Zudem zählen ein Lebenszyklus-Management, das automatisiert die Erstellung, Rotation und Löschung von Maschinenidentitäten steuert, sowie ein feingranulares Rechtemanagement, das Maschinenzugänge im Least-Privilege-Prinzip durchsetzt. Ziel ist die reibungslose Provisionierung und Rotation, wobei Zugriffsprotokollierung sicherstellen sollte, dass auch maschinelle Interaktionen nachvollziehbar bleiben. In dem Zusammenhang rückt nicht zuletzt die Integration mit dem CIEM (Cloud Infrastructure Entitlement Management), Secrets Management oder in DevSecOps-Pipelines in den Fokus.

## 1.2 Wildwuchs der Identity Provider (IdP)

Auch die Anzahl und Vielfalt von Identity Providern wächst kontinuierlich und wer als Unternehmen nicht den Anschluss verlieren möchte, muss in der Lage sein, mit einer Vielzahl interner und externer Identitätsquellen zu interagieren. Die Spanne reicht von lokalen Active Directories, Entra ID, Microsoft Azure Active Directory oder Google Identity über Behördenportale und Bank-Ident-Verfahren bis hin zu Social-Login-Möglichkeiten und neuen Wallet-basierten Ansätzen wie EUDI oder E-ID. Entsprechend ist die Realität von einer stark fragmentierten IAM-Landschaft mit unterschiedlichen Protokollen (OAuth2, OpenID Connect, SAML – Security Assertion Markup Language etc.), Trust-Niveaus und Verwaltungskonzepten geprägt. Multi-IdP-Anforderungen durch Parallelnutzung mehrerer Systeme gehen mit komplexen Authentifizierungsflüssen auf Basis vielfältiger Tokenformate, Claims-Standards und Vertrauensanker einher. Bei der Einbindung sollten Bruchstellen in der User Journey idealerweise von Anfang an vermieden werden. Entsprechend fallen abweichende Login-Erfahrungen je nach IdP durchaus ins Gewicht. Noch viel zu oft fehlt Konsistenz im Hinblick auf Onboarding, Login und Consent – ein Problem, das nicht nur hinsichtlich der Akzeptanzhürden auf Anwenderseite gelöst werden muss.

**«Wer heute nicht Multi-IdP-fähig ist, verliert morgen den Zugang zu den Benutzern oder wird regulatorisch ausgesperrt. Viele IAM-Systeme können mittlerweile mit Open ID Connect und SAML umgehen, aber nur wenige sind bereits auf EUDI, Self-Sovereign Identities (SSI) und Wallets vorbereitet.»**

## Anforderung

Multi-IdP-Fähigkeit gehört in jedem Fall zu den Grundvoraussetzungen effektiver Authentifizierungsprozesse. Ein Federation Layer – als Komponente in Datenmanagementsystemen, die es ermöglicht, Daten aus verschiedenen Quellen zu integrieren – oder ein entsprechend ertüchtigtes IAM-System sind wichtige Weichensteller für ein dynamisches IdP-Routing und bringen zusätzliche Flexibilität bei der Auswahl des geeigneten IdP (z.B. basierend auf Region, User-Typ und Verfügbarkeit). Zugleich gilt es, kontextsensitive Authentifizierung zu ermöglichen und zugrundeliegende Claim-Mappings und Trust-Policies so weit wie möglich zu standardisieren. Ziel muss die zentrale Authentifizierungssteuerung sein, die Trust-Brokering über ein einheitliches Consent Management und durchgängige Prozesse gewährleistet, inklusive transparenter Benutzerführung. Schliesslich darf die Komplexität der Providerlandschaft nicht zu Lasten des Endnutzers gehen.

## 1.3 Device- und Kanalvielfalt

Nutzer bewegen sich heute zwischen Smartphone, Laptop, Smart-TV, POS-Terminal und Wearable. Authentifizierung muss all diese Geräteklassen bedienen und entlang des Omnichannel-Ansatzes sowohl Webbrowser, native Apps und Embedded Devices als auch API und Konsolenanwendungen unter den Schutzschirm verlässlicher Verbindungen stellen – konsistent, sicher und nutzerfreundlich. Dies kann vor dem Hintergrund unterschiedlichster Eigenschaften einzelner Geräte und Anwendungen durchaus kompliziert werden. Schliesslich mag ein QR-Code am Desktop hilfreich sein, auf einem Smartphone eignet er sich aber nicht. Gleichzeitig stellen einzelne Clients andere Ansprüche im Hinblick auf passende Sicherheitsmodelle. Device-Binding als Sicherheitsmechanismus, der eine eindeutige Verbindung zwischen einem Gerät und einem Benutzerkonto oder einer Netzwerkrichtlinie herstellt, ist bei Weitem noch nicht flächendeckend verankert und von einem konsistenten Vorgehen über alle Kanäle hinweg sind zahlreiche Unternehmen noch deutlich entfernt.

**«Die Zeiten, in denen man alles im Browser lösen konnte, sind vorbei. Heute müssen Authentifizierungsprozesse auch für Smartphone, Tablet und Co. funktionieren. Wer keine kanalagnostische Authentifizierung umsetzt, kann immer nur einen Teil der Identität schützen.»**

### Anforderung

Abhilfe schaffen kanal- und gerätespezifische Authentifizierungsflows (z.B. via WebAuthn, QR-Login oder Magic Link), die im Einklang mit dynamischen Trust-Scores stehen. Standardisierung, wie sie beispielsweise FIDO2 (Fast Identity Online 2) bietet, trägt nachhaltig zur besseren Authentifizierung bei gleichzeitiger Gerätekontrolle bei. Fallback-fähige Alternativen sorgen für zusätzliche Flexibilität in Bezug auf Altsysteme ohne moderne Authentifizierungsschnittstellen. Responsive und barrierefreie User-Interface (UI)-Komponenten sind in dem Zusammenhang genauso wichtig wie Context-Awareness, um Anmeldevorgänge effektiv an das Gerät anzupassen (z.B. biometrische Anmeldung auf Mobilgerät, Passwort auf Desktop).



## 1.4 Kreativität der Angreifer

Das Mitgefühl der Angreifer angesichts der bereits beschriebenen Herausforderungen hält sich eher in Grenzen – vielmehr sehen sie genau darin ihren Vorteil und nutzen jede sich bietende Chance, um Authentifizierungsprozesse zu umgehen oder Lücken in ihrem Sinne auszuspielen. Die dabei an den Tag gelegte Kreativität überrascht immer wieder – insbesondere im Zuge von Phishing oder Man-in-the-Middle (MitM)-Angriffen. Es besteht mittlerweile kein Zweifel mehr daran, dass Passwörter die grösste Schwachstelle der Authentifizierung sind und bleiben – egal ob leicht zu erraten, immer wieder verwendet oder durch gezieltes Phishing erbeutet. Gerade in Kombination mit Social Engineering wächst die Gefahr des Datendiebstahls weiter und herkömmliche Multi-Faktor-Authentifizierung kann dem kaum etwas entgegensetzen. Viele MFA-Verfahren (z.B. per SMS oder E-Mail-Link) sind leicht zu kompromittieren und bieten keinen Schutz, wenn die Integrität der Kommunikationsstrecke erst einmal verletzt ist. Basierend auf der Tatsache, dass Phishing nach wie vor das Einfallstor Nummer eins bei Identity-basierten Angriffen darstellt, müssen Unternehmen ihre Abwehr konsequent ausrichten und auch neue Angriffsszenarien ins Kalkül ziehen. Der Ideenreichtum und die Perfidität der Gegenseite kennen kaum Grenzen: Session Hijacking und Consent Phishing sind hier nur einige Beispiele einschlägiger Methoden, die MitM-Attacken den Weg bahnen. Ein solches Vordringen ist nur schwer zu erkennen, die Attacken erfolgen oft über kompromittierte Netzwerke, manipulierte DNS (Domain Name System)-Auflösungen oder durch Reverse Proxies. Selbst sichere Kanäle sind angreifbar, wenn Session-Token abgefangen werden oder Replay-Angriffe möglich sind. Mit Werkzeugen wie EvilProxy ist es inzwischen sogar gelungen, FIDO2-geschützte Logins abzufangen. Insofern sollte sich kein Unternehmen unverwundbar fühlen. Es kommt mehr denn je darauf an, bestehende Zugangskontrollen immer wieder auf den Prüfstand zu stellen und gegebenenfalls für zusätzliche Absicherung zu sorgen.

**«Session Hijacking und Consent Phishing sind Paradebeispiele für die Perfidität der Cyberkriminellen. So klicken Nutzer per böartigem OAuth Consent Flow beispielsweise arglos auf <OK>, ohne überhaupt zu verstehen, was sie freigeben.»**

### Anforderung

Aufgrund immer ausgefeilterer Angriffsvarianten dürfen Authentifizierungsabläufe niemals aus dem Blick geraten. Phishing-resistente Authentifizierung ist das Gebot der Stunde und die Nutzung von Passkeys (FIDO2 mit Device-Binding) gewiss ein Best Practice, jedoch auch nicht der Weisheit letzter Schluss. Es ist wichtig, die Authentifizierungslogik konsequent an neue Notwendigkeiten anzupassen und Kontextdaten zu berücksichtigen: Denn nur weil ein Login technisch korrekt ist, heisst das nicht, dass er legitim ist. Risikobasierte, adaptive Authentifizierung oder Continuous Adaptive Trust tragen dazu bei, das Risiko laufend zu kontrollieren. Sobald das Risikoniveau zu hoch wird, ist es von Vorteil, wenn sich zusätzliche Prüfläufe zielgenau ergänzen lassen. Darüber hinaus muss das Augenmerk auf der Aufklärung der Nutzer liegen. Weitere Weichensteller sind die Analyse durch Fraud & Anomaly Detection, Session-Protection-Strategien in Form von Token mit kurzen Gültigkeiten oder automatischer Session-Rotation sowie Massnahmen zur Härtung der Transportkanäle wie TLS-Zertifikats-Pinning, DNSSEC (Domain Name System Security Extensions) und HSTS (HTTP Strict Transport Security).



## 1.5 KI-Einsatz

An die Ausführungen zur zunehmenden Kreativität der Angreifer schliesst sich der Verweis auf die Popularität von Künstlicher Intelligenz (KI) nahtlos an. Denn Cyberkriminelle haben den Mehrwert von KI als Wunderwaffe ganz sicher erkannt. KI kann biometrische Merkmale wie Stimme, Gesicht oder Verhalten täuschend echt nachahmen und so biometrische Authentifizierungen gekonnt unterwandern. Die Folge: der nachhaltige Vertrauensverlust gegenüber traditionellen Authentifizierungsmerkmalen und ein wachsender Anspruch im Hinblick auf die technischen Fähigkeiten von IAM-Systemen, mit unsicheren Kontextdaten umzugehen und Misstrauen zu bewerten. Die mit KI einhergehenden Risiken werden dabei künftig immer grösser: Schon heute sind KI-gestützte Bots in der Lage, massenhaft Login-Versuche durchzuführen, Elemente der Benutzerschnittstellen zu erkennen und sogar Captchas zu lösen. Nicht zu vergessen die neuen Möglichkeiten von generativer KI, mit denen es Angreifern im Handumdrehen gelingt, im Zuge von Social Engineering überzeugende Phishing-Mails, Login-Seiten oder Support-Chats zu simulieren – massgeschneidert und skalierbar. Die KI-Gefahr droht aber nicht nur von aussen, sondern auch unternehmensintern in Form von Schatten-IT. Denn immer mehr Mitarbeitende nutzen ebenfalls KI-Tools wie ChatGPT, Perplexity, Claude, Copilot oder Midjourney auch in automatisierten Prozessen. Eine zentrale Identitätssteuerung oder Sicherheitskontrolle sucht man dabei meist vergebens, da viele dieser Dienste keine unternehmensweiten Single Sign-On (SSO)- oder cIAM-Standards unterstützen. Auf diese Weise entstehen und agieren zahlreiche Identitäten ausserhalb des geschützten Rahmens.

**«Generative KI hat die Hürden für professionelles Phishing massiv gesenkt. Gut formulierte Phishing-Mails sind heute an der Tagesordnung. Früher erkannte man 9 von 10 Täuschungsversuchen, das ist heute kaum mehr möglich. Und auch Onboarding-Prozesse, die Videoident nutzen, werden mit KI und Deepfakes inzwischen zum Katz-und-Maus-Spiel.»**

### Anforderung

KI ist gekommen, um zu bleiben. Somit ist die Etablierung neuer Sicherheitsmodelle für eine KI-native Welt von entscheidender Bedeutung. Es zählen Verhaltensanalysen in Echtzeit, bei denen der Fokus nicht allein auf biometrischen Mustern, sondern ebenso auf deren Konsistenz liegt. Statt blosser Erkennung geht es um stichhaltige Verifikation (z.B. Challenge-Response vs. statische Matching-Verfahren) und kontinuierliche Authentifizierung, die anstelle von Einmalprüfungen tritt. Es kommt darauf an, einem Vertrauensverlust konsequent entgegenzuwirken. Neben der bereits angesprochenen Phishing-resistenten Authentifizierung sollte daher das Augenmerk insbesondere auch auf einer stärkeren API-Sicherheit für Machine-to-Machine-Verkehr liegen. Zudem ist es auf Unternehmensseite ratsam, Zugriffskontrolle ebenso für KI-Plattformen und -Tools zu ermöglichen.

## 1.6 Quantencomputing

Bei diesem Thema handelt es sich bei Weitem nicht mehr um Zukunftsmusik und die rasante Entwicklung der Quantencomputer-Technologie wird traditionelle Verschlüsselungsverfahren über kurz oder lang vor neue Herausforderungen stellen. Quantencomputer nutzen das Prinzip der Superposition und Verschränkung, wodurch sie viele Berechnungen gleichzeitig durchführen können. Ein leistungsstarker Quantencomputer ist in der Lage, die Faktorisierung grosser Primzahlen – als Grundlage der RSA-Verschlüsselung (benannt nach den Kryptografen Rivest–Shamir–Adleman) – extrem schnell zu bewerkstelligen. Der sogenannte Shor-Algorithmus ermöglicht es, die Sicherheit traditioneller Verschlüsselungen innerhalb von Stunden oder sogar Minuten zu überwinden, während dies mit klassischen Computern Millionen von Jahren dauern würde. Die Kryptografie steht somit unter Druck. In der Ära der Quantencomputer mutiert die gängige asymmetrische Verschlüsselung wie RSA oder ECC (Elliptic Curve Cryptography) zum zahnlosen Tiger. Dabei ist die Gefahr bereits heute allgegenwärtig. Schon jetzt werden einschlägige Daten abgefangen und gespeichert mit der Erwartungshaltung, diese in absehbarer Zeit mit Quantenpower entschlüsseln zu können. Riskant ist dies vor allem im Rahmen von TLS-Verbindungen (Transport Layer Security), die in der Kommunikation zwischen Webbrowsern und Servern verwendet werden. Aber auch für VPN-Tunnel und verschlüsselte E-Mails, die auf asymmetrische Kryptografie setzen, sowie digitale Signaturen, die bei Authentifizierung und Transaktionen im Finanzwesen Wirkung entfalten, ist die Gefahr offensichtlich. Standards für die Post-Quantum-Ära sind seitens der US-Forschungseinrichtung NIST (National Institute of Standards and Technology) zwar in Arbeit, die Unsicherheit bleibt aber nach wie vor gross. Viele Unternehmen wissen nicht, wann und wie sie reagieren sollen – zumal ein Nachrüsten augenscheinlich mit zusätzlichen Problemen einhergehen könnte, da PQC (Post-Quantum Cryptography)-Verfahren rechenintensiv, schwer in Legacy-Systeme integrierbar und nicht immer interoperabel sind.

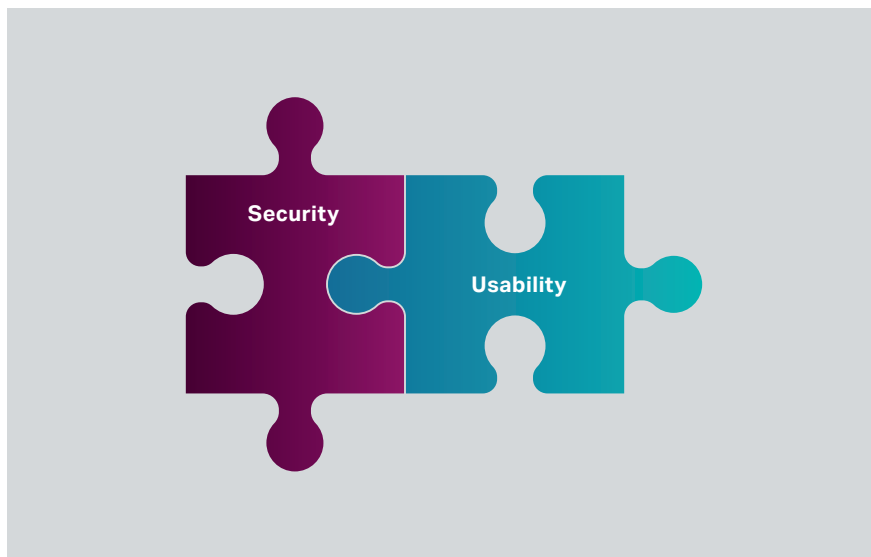
**«Wenn man die potenzielle Gefahr von Quantencomputing einfach ignoriert und nicht mindestens abklärt, was es zu tun gibt, dann hat man in ein paar Jahren ein böses Erwachen.»**

### Anforderung

IAM-Systeme, die heute aufgebaut oder modernisiert werden, müssen «post-quantum ready» sein – nicht, weil Quantencomputer morgen einsatzfähig sind, sondern weil Identitätsdaten oft eine lange Schutzdauer erfordern. Daher sollten sich die Verantwortlichen rechtzeitig mit den Aspekten der Risikobewertung und Migrationsstrategie für kryptografische Assets (z.B. X.509-Zertifikate, TLS, Token-Signaturen) auseinandersetzen. Die Etablierung hybrider Kryptografie als Kombination aus klassischer und quantensicherer Verschlüsselung (mithilfe quantenresistenter Algorithmen wie CRYSTALS-Kyber) kann den Übergang erleichtern. Insofern gilt es, die PQC-Readiness im IAM und cIAM zu prüfen – insbesondere im Hinblick auf JWT (JSON Web Token), SAML (Security Assertion Markup Language)- oder OIDC (Open ID Connect)-Flows. Unternehmen, die schon jetzt wissen, welche Produkte, IdP und Komponenten PQC-kompatibel sind, erarbeiten sich einen strategischen Vorteil. Durch Algorithmus-Agilität ergibt sich die Chance, neue Verschlüsselungsstandards einzuführen, ohne die komplette Plattform zu tauschen. Ein gezieltes Monitoring bei der Verwendung kritischer Schlüssel trägt dazu bei, Bedrohungspotenziale frühzeitig zu erkennen. Da Interoperabilität nicht zuletzt von der Einhaltung spezifischer Standards abhängig ist, sollte zudem von Anfang an auf Einhaltung und Etablierung von NIST-zertifizierten Algorithmen oder Empfehlungen des Europäischen Instituts für Telekommunikationsnormen (ETSI) geachtet werden.

## 1.7 Wettbewerbsfaktor Benutzerfreundlichkeit

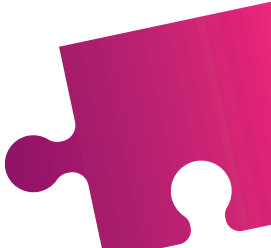

Die Aufgabenliste der Verantwortlichen für Identitäts- und Zugriffsmanagement ist angesichts all dieser Herausforderungen schon jetzt schwer überschaubar. Gleichzeitig schwebt über allem Engagement das Gebot maximaler Anwenderfreundlichkeit. Denn was bringt es, wenn die Authentifizierungsprozesse zwar höchste Sicherheit gewährleisten, aber die Abläufe auf Seiten der Mitarbeitenden und Kunden zum Aufgeben führen? Es darf niemals ausser Acht gelassen werden, dass zusätzliche Sicherheitsmassnahmen die kognitive Last erhöhen oder die User Journey verlangsamen können. So steht beispielsweise der Geschäftserfolg auf dem Spiel, wenn Kunden im Zuge von Multi-Faktor-Authentifizierung zu viele Schritte durchlaufen müssen und abrechnen. Gerade im Onboarding-Prozess ist dies ein besonders kritischer Punkt. Ein weiteres Risiko bergen Szenarien, in denen Nutzer die Sicherheitsvorkehrungen umgehen, sich gegebenenfalls über unautorisierte Tools behelfen und dabei weiterhin schwache Passwörter verwenden. Insofern ist es umso wichtiger, in jederlei Hinsicht den Brückenschlag zwischen Sicherheit und Benutzerfreundlichkeit zu schaffen. Denn diese beiden Puzzleteile sollten für eine erfolgreiche cIAM-Strategie auf alle Fälle zusammenpassen.




**«Je besser die Angreifer das Spiel der User Experience (UX) verstehen, desto gefährlicher werden sie.»**

### Anforderung

Usability ist ein kaum zu unterschätzender Faktor bei der Ausgestaltung von Sicherheitskonzepten. Klaren Mehrwert bringen in dem Zusammenhang nutzerzentrierte Authentifizierungsflüsse und ein adaptiver und kontextbasierter Ansatz der Authentifizierung, der nur dann zusätzliche Authentifizierungsstufen vorsieht, wenn es das Risiko verlangt. Details können bei der Multi-Faktor-Authentifizierung einen grossen Unterschied ausmachen und sie nahezu unsichtbar erscheinen lassen. Gute Beispiele dafür sind Device Fingerprinting, In-App-Push mit Biometrie oder Silent Re-Authentication via Single Sign-On (SSO). Darüber hinaus bieten Self-Service-Funktionen (z.B. zur Passwortzurücksetzung) schnelle Hilfe und sorgen nicht zuletzt für Entlastung von Helpdesks.



**Durch die *hohe Benutzerfreundlichkeit* haben wir für unsere Kunden eine eindeutige Raiffeisen-Identität geschaffen. Kundennähe und *Vertrauenswürdigkeit* haben bei uns oberste Priorität.**



**Stevan Dronjak,**  
Team Lead Web Application Security  
Raiffeisen Schweiz

**RAIFFEISEN**

Die richtige Kombination von Security und Benutzerfreundlichkeit schafft Vertrauen beim Kunden.

Quelle: Airlock



## 2. Relevante Puzzleteile im Zuge steigender Anforderungen

Die Umsetzung moderner, identitätsbasierter Sicherheit ist eine Aufgabe, bei der vielfältige Anforderungen zum Tragen kommen. Beim Identitäts- und Zugriffsmanagement müssen verschiedenste Funktionalitäten wie die Teile eines Puzzles sinnvoll ineinandergreifen, um ein stimmiges Gesamtbild zu ergeben. Einige Leistungsbausteine und Technologien sind dabei besonders zentral, da sie den Rahmen schaffen, den es im weiteren Verlauf gezielt auszufüllen gilt – eben wie bei einem Puzzle die Randteile. Um Klarheit in den Dschungel der Aufgaben zu bringen, sind im Folgenden die Themen aufgeführt, die Verantwortliche für Identitäts- und Zugriffsmanagement zwingend im Blick haben sollten. Denn sie bilden das Fundament, um aktuellen und zukünftigen Herausforderungen erfolgreich zu begegnen. Den strategischen Stellenwert der einzelnen Bausteine sowie ihre Auswirkungen auf Sicherheit und Nutzerfreundlichkeit veranschaulicht jeweils die Legende.



## 2.1 Passwortlose Authentifizierung

Dringlichkeit ▲▲▲

Security ✓✓✓

Nutzerfreundlichkeit ♥♥♥



Passwortlose Authentifizierung verzichtet vollständig auf herkömmliche Passwörter und setzt stattdessen auf Alternativen wie FIDO2, biometrische Verfahren (Fingerabdruck, Gesichtserkennung), Hardware-Token oder sogenannte Magic Links. Durch die Eliminierung unsicherer Passwörter sinkt vor allem die Gefahr von Datenlecks und Identitätsdiebstählen drastisch.

Aus Nutzersicht sind passwortlose Lösungen intuitiv, schnell und komfortabel. Kunden müssen sich keine komplizierten Passwörter merken, was die Nutzererfahrung wesentlich verbessert. Unternehmen profitieren von einer erhöhten Akzeptanz ihrer digitalen Services und reduzieren gleichzeitig Supportaufwände für Passwort-Rücksetzungen erheblich.

Entsprechend sollte die einfache und sichere Integration passwortloser Verfahren in bestehende IT- und Sicherheitsinfrastrukturen mit Nachdruck vorangetrieben werden. Genau hier verbirgt sich ein entscheidender Hebel, um Sicherheit und Nutzerfreundlichkeit optimal in Einklang zu bringen. Als State-of-the-Art gilt die Umsetzung einer Phishing-resistenten Authentifizierung auf Grundlage des FIDO2-Standards.

### 2.1.1 FIDO2 als Allheilmittel?

Dringlichkeit ▲▲

Security ✓✓

Nutzerfreundlichkeit ♥♥



FIDO2 wurde von der FIDO-Allianz (Fast Identity Online) und dem World Wide Web Consortium (W3C) entwickelt, um Logins ohne Passwort sicher und einfach zu machen. Statt wie üblich ein Passwort einzugeben, bestätigt der Nutzer seine Anmeldung direkt auf seinem Gerät – etwa per Fingerabdruck oder Gesichtserkennung. Die technische Grundlage dahinter: eine gesicherte Verbindung zwischen Gerät und Dienst, bei der keine sensiblen Daten übertragen werden. So bleiben Login-Daten vor Phishing oder Diebstahl geschützt.

Dank sogenannter Passkeys – sicheren Login-Informationen, die über alle persönlichen Geräte hinweg synchronisiert werden – funktioniert dieser Ansatz heute bereits für Hunderte Millionen Menschen. Grosse Plattformen wie Amazon und Google zeigen, wie erfolgreich passwortlose Logins sein können: In den letzten zwei Jahren stieg die Erfolgsrate beim Login um 30 %, der Anmeldeprozess wurde im Schnitt 20 % schneller.



**Beispiel:** Ein praktisches Beispiel für FIDO2 ist die Anmeldung bei einem E-Banking-Portal mittels Fingerabdruckscan: Der Kunde wählt «Mit Gerät anmelden», erhält eine Push-Benachrichtigung oder verwendet sein Gerät, um den Fingerabdruck zu scannen. Im Hintergrund signiert sein Smartphone die Login-Challenge des Bankservers mit dem privaten Schlüssel, der im Tresor des Telefons gespeichert ist. Der Bankserver prüft die Signatur mit dem zugeordneten öffentlichen Schlüssel und lässt den Zugriff zu – ohne dass der Kunde je ein Passwort eingeben musste. Selbst wenn Phishing-Betrüger ihm eine gefälschte Bankseite präsentieren würden, könnten sie diesen Anmeldevorgang mangels eines privaten Schlüssels nicht replizieren.

Durch Unterstützung von FIDO2/WebAuthn in Kundenportalen kann die Sicherheit signifikant erhöht werden – Angriffe via Phishing, Credential Stuffing oder passwortbezogenem Datenleck laufen ins Leere – bei gleichzeitiger Verbesserung der User Experience.

FIDO2 gilt als Goldstandard für sichere, benutzerfreundliche Authentifizierung. Nichtsdestotrotz darf es nicht als Allheilmittel verstanden werden. Besonders bei Maschinenidentitäten, Legacy-Systemen oder hybriden Infrastrukturen stösst FIDO2 an Grenzen. Eine sinnvolle Koexistenz mit anderen Verfahren ist notwendig – ebenso wie eine starke Orchestrierung, Kontextbewertung und Risikosteuerung im Hintergrund.

## 2.2 Risikobasierte Authentifizierung

Dringlichkeit 

Security 

Nutzerfreundlichkeit 



Risikobasierte Authentifizierung (Risk-Based Authentication, RBA) hat zum Ziel, Sicherheit und Benutzerfreundlichkeit in Einklang zu bringen. Das etablierte Sicherheitskonzept steuert den Zugriff auf digitale Anwendungen dynamisch auf Basis einer kontinuierlichen Risikobewertung. Dabei werden in Echtzeit verschiedene Faktoren analysiert – etwa ob sich ein Nutzer aus einem ungewöhnlichen oder risikobehafteten Land anmeldet, ob ein bekanntes oder neues Gerät verwendet wird, ob der Login-Zeitpunkt vom üblichen Verhalten abweicht oder ob das Nutzungsmuster insgesamt als auffällig eingestuft wird. Aus diesen Informationen wird ein Risikowert ermittelt, der entscheidet, ob der Zugang gewährt, eine zusätzliche Authentifizierung verlangt oder der Zugriff blockiert wird.

Die Vorteile der risikobasierten Authentifizierung sind somit schnell auf den Punkt gebracht: Mithilfe von RBA können Anomalien sofort erkannt und unautorisierte Zugriffe noch besser verhindert werden. Da sich die Sicherheitsanforderungen automatisch dem Risikoprofil der jeweiligen Sitzung anpassen, werden zusätzliche Prüfläufe nur dann nötig, wenn es die konkrete Situation erfordert. Legitimen Nutzern wird der Zugang ohne zusätzliche Hürden ermöglicht.

**Beispiel:** Banken nutzen risikobasierte Authentifizierung, um bei Anmeldungen aus fremden Ländern oder ungewöhnlichen Transaktionen zusätzliche Sicherheitsabfragen zu stellen. Im Versicherungsbereich werden risikobehaftete Zugriffe auf sensible Daten mit einer zusätzlichen Multi-Faktor-Authentifizierung (MFA) abgesichert.

## 2.3 Continuous Adaptive Trust

Dringlichkeit ▲▲▲

Security ✓✓✓

Nutzerfreundlichkeit ♥♥♥



Das Konzept von Continuous Adaptive Trust ist die logische, fortschrittlichere Ergänzung der risikobasierten Authentifizierung. Im Gegensatz zu klassischen Authentifizierungsmethoden, die nur einmalig beim Login eine Identitätsprüfung vornehmen, verfolgt Continuous Adaptive Trust einen ganzheitlichen Ansatz. Das Verhalten des Nutzers wird während der gesamten Sitzung analysiert und bei Anomalien werden Zugriffe eingeschränkt oder zusätzliche Authentifizierungen gefordert. Erkennt das System auffälliges Verhalten, wie z.B. einen plötzlichen Standortwechsel, wird die Sicherheitsstufe automatisch erhöht. Faktoren wie Geolocation, Geräteinformationen und Nutzungsverhalten werden fortlaufend im Blick behalten, um das Risiko lückenlos bewerten zu können. Der Nutzer merkt im Normalfall nichts von der Überwachung, solange keine Auffälligkeiten auftreten.

**Beispiel:** Eine Mitarbeiterin oder ein Mitarbeiter meldet sich über VPN im Firmennetzwerk an und wechselt plötzlich seinen Standort um tausende Kilometer. Das System erkennt diese Änderung und fordert eine erneute Authentifizierung oder blockiert den Zugriff. In Versicherungen können Kunden, die sensible Dokumente abrufen, während der gesamten Sitzung überprüft werden, um sicherzustellen, dass keine unautorisierten Änderungen vorgenommen werden.

## 2.4 SSI-Enablement

Dringlichkeit ▲▲▲

Security ✓✓✓

Nutzerfreundlichkeit ♥♥♥

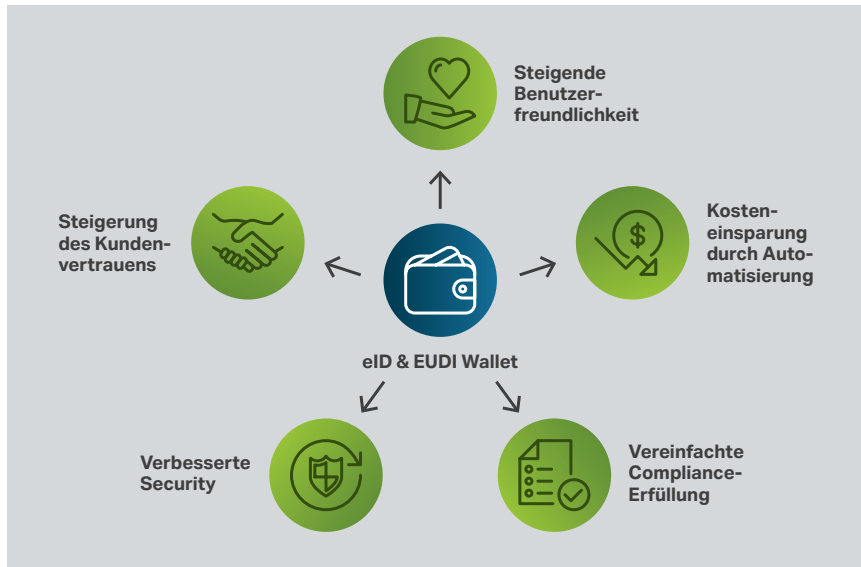


In die vielfältige Landschaft der Identitätsprovider kommt mit den aktuellen gesetzlichen Initiativen rund um dezentrale Identitäten (Self-Sovereign Identity, SSI) ganz neuer Schwung. Die Europäische Digitale Identität (EUDI) – oder E-ID in der Schweiz – ist ein ehrgeiziges Projekt der Europäischen Union, das auf Basis von SSI eine einheitliche, interoperable und sichere digitale Identität für alle Bürgerinnen und Bürger der EU bereitstellen soll. Im Rahmen des europäischen «Digital Identity Framework» soll es die EUDI ermöglichen, sich online eindeutig zu identifizieren und rechtsverbindliche Transaktionen durchzuführen – länderübergreifend und vollständig digital. Nutzer behalten dabei die Kontrolle über ihre persönlichen Daten und bestimmen selbst, welche Informationen geteilt werden. Auf diese (R)Evolution der digitalen Identität<sup>2</sup> müssen Unternehmen vorbereitet sein. Es ergeben sich komplett neue Wege zur digitalen Identifikation – ohne Umwege über zentrale Dienste (wie Google oder Apple). Digitale Souveränität lautet hier das entscheidende Schlagwort. Verbindliche Gesetze, die Behörden und Unternehmen zur Umsetzung von SSI verpflichten, stehen kurz bevor und werden Hunderten Millionen Menschen moderne Möglichkeiten zum Identitätsnachweis und zur Datenautorisierung bieten.

Daher muss eine cIAM-Lösung SSI in naher Zukunft abbilden können. Die erfolgreiche Implementierung erfordert neben der Gewährleistung von Interoperabilität mit bestehenden Authentifizierungsmethoden und hohen Sicherheitsstandards für den Datenschutz vor allem die nahtlose Integration in digitale Services.

**Beispiel:** Ein Anwendungsfall im Bankenbereich ist die Authentifizierung von Kunden bei Finanztransaktionen. Durch die Vorlage eines digitalen, verifizierten Identitätsnachweises (E-ID, EUDI-Wallet) kann sich ein Kunde sicher und zuverlässig gegenüber der Bank authentifizieren – ohne klassische Benutzerkonten oder Passwörter. Im öffentlichen Bereich ermöglicht SSI den Zugang zu behördlichen Dienstleistungen, ohne dass zentrale Identitätsregister abgefragt werden müssen. Bürger können beispielsweise eine digitale Bürger-ID als Verifiable Credential vorlegen, um auf Services wie Steuerportale oder Anwendungen rund um Sozialleistungen zuzugreifen.

<sup>2</sup> Whitepaper «Die (R)Evolution der digitalen Identität», Airlock, URL: <https://www.airlock.com/whitepaper-die-revolution-der-digitalen-identitaet>



Dezentrale Identitäten und der korrekte Umgang mit EUDI und E-ID bringen nicht nur Vorteile für den Anwender, sondern auch für Unternehmen, die rechtzeitig die Vorbereitungen treffen.

Quelle: Airlock

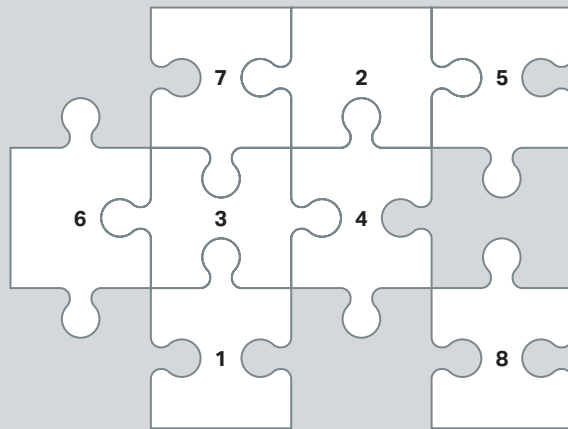
## 2.5 Post-Quanten-Kryptografie

Dringlichkeit ▲ Security ✓✓✓ Nutzerfreundlichkeit



Selbst wenn die Bedrohung durch Quantencomputing aktuell noch wenig greifbar ist, darf das Thema Post-Quanten-Kryptografie (PQC) an dieser Stelle nicht fehlen. Bestehende Authentifizierungsmethoden sind eventuell schneller als gedacht nicht mehr sicher genug. Und schon heute geht von «Harvest now, decrypt later»-Szenarien eine alarmierende Wirkung aus. Wenn Angreifer bereits jetzt verschlüsselte Daten abfangen und speichern, um sie später zu entschlüsseln, gilt es eher heute als morgen, tragfähige Strategien zu erarbeiten, um gerade Systeme mit sensiblen Informationen – wie Kundendaten, Authentifizierungsinformationen oder Geschäftsgeheimnisse, die durch kryptographische Verfahren geschützt werden – frühzeitig auf Post-Quanten-Kryptographie vorzubereiten. Der Begriff umfasst dabei verschiedene quantencomputerresistente Optionen, darunter beispielsweise gitter- oder codebasierte Kryptografie. Hybride Ansätze, bei denen klassische und quantensichere Algorithmen kombiniert werden, ermöglichen eine reibungslose Übergangsphase. Unternehmen können PQC so frühzeitig testen und nahtlos in ihre IT-Infrastruktur integrieren, ohne die Stabilität bestehender Systeme zu gefährden.

# 3. Best Practices: Die Bauanleitung für das Puzzle moderner Authentifizierung



- 1 Unterstützung offener Standards
- 2 Flexible Flows
- 3 Effiziente Migration von Authentifizierungsmitteln
- 4 Unterstützung von Token Exchange
- 5 Integration von SSI
- 6 Zusammenarbeit mit WAAP-Systemen
- 7 Identity Federation und hybride Landschaften
- 8 Nähe zum Kunden und digitale Souveränität

Die Anforderungen im Hinblick auf Authentifizierung und den effektiven Umgang mit digitalen Identitäten gehen inzwischen weit über den ursprünglichen Wirkungsbereich einer IAM-Lösung hinaus. Nichtsdestotrotz bildet das IAM-System im Allgemeinen – und das cIAM im Speziellen – das Rückgrat aller damit zusammenhängenden Prozesse. Ein flexibles cIAM-System ist der zentrale Baustein für eine zukunftsorientierte Identitätsarchitektur. Es muss nicht nur aktuelle Herausforderungen adressieren, sondern auch Raum für neue Entwicklungen lassen – von Post-Quantum-Kryptografie über EUDI bis hin zu KI-gestützten Sicherheitsmechanismen. Der Handlungsdruck ist da. Damit sich Unternehmen zukunftsfähig aufstellen können, sollte auf die folgenden acht Aspekte in besonderem Masse geachtet werden:

## Unterstützung offener Standards

Ein zukunftssicheres cIAM-System setzt auf etablierte Protokolle wie OAuth 2.0, OpenID Connect, SAML und FIDO2. Diese sorgen nicht nur für Interoperabilität mit bestehenden und zukünftigen Systemen, sondern ermöglichen auch eine nahtlose Integration in hybride und föderierte Identitätslandschaften. Die Zeiten sukzessive zusammengebastelter Infrastrukturen, die nicht nur mit hohem Integrationsaufwand und Kosten einhergehen, sondern sich darüber hinaus meist deutlich anfälliger gegenüber Angriffen präsentieren, sind passé. Es zählen Modularität und Standardisierung – im Sinne höchster Sicherheit.

## Airlock-Praxis

Für Airlock sind offene Schnittstellen nicht die Kür, sondern Pflicht. Zudem werden seit jeher Low-Code-/No-Code-Prinzipien verfolgt. Die IAM-Lösung unterstützt alle wichtigen Standards und fügt sich sowohl funktional als auch architektonisch in moderne, heterogene Identity-Konzepte ein.

Das Kundenportal des Schweizer Krankenversicherers [Visana](#) gilt bis heute als eines der kundenfreundlichsten Online-Portale der Schweiz und überzeugt vor allen in punkto Benutzerfreundlichkeit, Funktionalität und Systemstabilität. Dahinter steht eine kohärente Sicherheitsarchitektur, die es erlaubt, neue Services zu lancieren und in ein IT-Ökosystem zu integrieren, ohne sich im Nachhinein um die Sicherheit kümmern zu müssen. Der grosse Vorteil für das Unternehmen: deutlich kürzere Innovationszyklen und schnellere Time-to-Market-Prozesse. Dank der Security-Lösung von Airlock mit vorgelagertem API Security Layer können Web-Applikationen, mobile Anwendungen sowie eigene oder fremde APIs verlässlich integriert werden. Über offene Schnittstellen lassen sich Drittservices wie z.B. externe Gesundheits-Apps und Fitness-Tracker konvergent und zukunftssicher anbinden.

## Flexible Flows

Individuelle Customer Journeys erfordern flexible und konfigurierbare Authentifizierungs- und Autorisierungsflüsse. Ein cIAM-System sollte es ermöglichen, diese Flows kontextabhängig zu gestalten – etwa risikobasiert, rollenbasiert oder je nach Endgerät. Damit wird Sicherheit nicht zum Hindernis, sondern zum integralen Bestandteil eines guten Nutzererlebnisses.

## Airlock-Praxis

Airlock unterstützt durch seine flexible Flow-Architektur die nahtlose Integration heterogener IdP-Landschaften bei gleichzeitiger Berücksichtigung der Device- und Kanalvielfalt. Unternehmen können damit festlegen, über welchen Provider sich welche Nutzergruppen wie authentifizieren (etwa Biometrie auf dem Smartphone oder 2FA bei unbekanntem Gerät), wie Fallback-Mechanismen greifen und wie sich regulatorische Vorgaben pro IdP umsetzen lassen. Das schafft Interoperabilität ohne Kontrollverlust.

Ein perfektes Beispiel für die Umsetzung flexibler, individuell konfigurierbarer Authentifizierungsflüsse liefert das zentrale Secure Portal bei der [Johanniter-Unfall-Hilfe](#). Dieses ermöglicht über 60.000 Mitarbeitenden aus unterschiedlichen Landesverbänden mit vielfältigen Zugriffsberechtigungen spezifischen Zugang zu den jeweils erforderlichen IT-Anwendungen – ganz unabhängig vom verwendeten Endgerät. Dabei setzt der Secure Access Hub als integrierte Gesamtlösung mit WAF, API Gateway und cIAM auf eine starke Authentifizierung, bei der Zugriffe risikobasiert und adaptiv für verschiedene User-Gruppen gewährt werden. So sind sensible Personendaten jederzeit umfassend geschützt. Um den Spagat zwischen Security und Usability zu schlagen, werden Anwender im Zuge der Zwei-Faktor-Authentifizierung (2FA) über Push-Nachrichten und Smartphone identifiziert. Damit ist auch im Notfall der einfache Zugang zu wichtigen Daten sichergestellt. Eine weitere Besonderheit waren im konkreten Fall die unterschiedlichen Compliance-Anforderungen. So haben nicht nur die einzelnen Bundesländer und Gemeinden, sondern auch die Evangelische Kirche Deutschland, der die Johanniter unterstellt sind, ein eigenes Datenschutzgesetz (DSG-EKD). Dank des performanten Airlock IAM konnten alle Anforderungen zuverlässig erfüllt werden.

## Effiziente Migration von Authentifizierungsmitteln

Der Übergang von Passwörtern hin zu stärkeren Verfahren wie FIDO2 oder biometrischen Authentifizierungsmechanismen erfordert Planung. Best Practices umfassen die parallele Unterstützung alter und neuer Verfahren, ein gezieltes Risikomanagement sowie schrittweises Onboarding mit Ausrichtung auf hohe Benutzerfreundlichkeit.

### Airlock-Praxis

Mit effektiver, risikobasierter Authentifizierung und Continuous Adaptive Trust liefert Airlock das Fundament resilienter Prozesse. Nicht nur das Gefahrenpotenzial wird dadurch besser kontrollierbar. Zudem werden Unternehmen in die Lage versetzt, das Sicherheitsniveau angesichts der jeweiligen Bedrohungslage konsequent anzupassen. Darüber hinaus stellt Airlock schon heute die Weichen für die Integration kryptografischer Verfahren, die auf Post-Quanten-Kryptografie vorbereitet sind. Die Plattform ermöglicht eine schrittweise Migration, indem hybride Modelle verwendet werden, die klassische Verschlüsselung mit quantensicheren Algorithmen kombinieren. Schlüsselmanagement und Authentifizierungslogik sind dabei klar getrennt. So können Unternehmen ihre cIAM-Architekturen zukunftssicher gestalten, ohne bestehende Sicherheitsstandards zu gefährden. Im Zuge von User Self Services erleichtert Airlock nicht zuletzt einen einfachen und kostengünstigen Rollout neuer Authentifizierungsverfahren gegenüber den Anwendern.

Wie schnell und einfach der Umstieg auf eine verlässliche und moderne Zwei-Faktor-Authentifizierung gelingen kann, zeigt das Projekt bei der [Frankfurter Bankgesellschaft \(Schweiz\) AG](#). Über die integrierte Gesamtlösung von Airlock, die in Kombination von Secure Access Hub und cIAM eine zentrale und vorgelagerte Verwaltung aller Benutzer- und Zugriffsrechte ermöglicht, war die Ablösung der bisherigen RSA-Token-basierten Authentifizierung zügig umgesetzt. An deren Stelle trat in kürzester Zeit die nutzerfreundliche und weitaus verlässlichere passwortlose One-Touch-Zwei-Faktor-Authentifizierung. Durch nahtlose Authentisierungs-Flows mit Single Sign-On wird nicht nur Usability-Ansprüchen nachhaltig Rechnung getragen, sondern gleichzeitig die IT-Abteilung entlastet, da sich passwortbezogene Probleme in Luft auflösen. Der Zugriff erfolgt absolut sicher und nachvollziehbar, was gerade in Branchen mit strengen Compliance-Anforderungen ein entscheidendes Argument ist.

## Unterstützung von Token Exchange

Token Exchange erlaubt es, Identitätsinformationen zwischen verschiedenen Systemen sicher zu übertragen – etwa von externen IdP zu internen Diensten. Dies ist essenziell für komplexe Integrationsszenarien in grossen Organisationen und fördert die Wiederverwendbarkeit bestehender Identitäten.

### Airlock-Praxis

Airlock Secure Access Hub integriert technische Konzepte wie Token Exchange, mandantenfähige API-Authentifizierung und Policy Enforcement Points (PEP), die auch nicht-menschliche Identitäten sicher durch den Authentifizierungsprozess schleusen. In Kombination mit Secrets Management und Just-in-Time-Berechtigungen (z.B. über Vaults oder CIEM-Systeme) ergibt sich ein schlüssiges Sicherheitsmodell, das auch in der dezentralen Kubernetes-Welt und in hybriden Cloud-Umgebungen greift.

Auf Basis von OAuth 2.0 Token Exchange ist die [Schweizerische Bundesbahnen AG](#) in der Lage, mehrere hundert Service-Anbieter sicher auf einer Plattform zu integrieren. Das Prinzip: mehrfache Sicherheit dank gezielter Segmentierung. 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 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.

## Integration von SSI

Self-Sovereign Identity (SSI) ermöglicht Nutzern die volle Kontrolle über ihre digitalen Identitäten. Moderne cIAM-Systeme sollten SSI-Konzepte und die Verifikation von Verifiable Credentials unterstützen, um neue Vertrauensmodelle zu fördern – besonders im Kontext von EUDI, E-ID und damit einhergehenden regulatorischen Entwicklungen.

### Airlock-Praxis

Die nahtlose Integration von SSI-Technologien in bestehende cIAM-Landschaften bereitet mit Airlock keinerlei Probleme. Durch die flexible Architektur der Plattform können Verifiable Credentials einfach in Authentifizierungsprozesse eingebunden werden. Die Sicherheitsmechanismen von Airlock sorgen dafür, dass diese digitalen Nachweise manipulationsicher und vertrauenswürdig eingesetzt werden können. Darüber hinaus bietet Airlock eine zentrale Managementoberfläche, über die Berechtigungen und Identitätsnachweise effizient administriert werden können. Damit lässt sich SSI nicht nur technisch sicher umsetzen, sondern auch operativ optimal verwalten.

In Vorbereitung auf SSI bietet Airlock bereits seit 2024 [Ideation Workshops](#) an. In diesen können Unternehmen herausfinden, welche konkreten Chancen sich für das eigene Tagesgeschäft ergeben. Aber auch die Risiken, die drohen, wenn man nicht rechtzeitig anfängt, werden im Zuge eines solchen Workshops gezielt veranschaulicht. Entlang der Darstellung konkreter Beispiele geht es vor allem darum, neue Ideen zu entwickeln, mit denen der Erfolg der individuellen Geschäftsmodelle auf Unternehmensseite vor dem Hintergrund des SSI-Siegeszugs künftig weiter gesteigert werden kann. Der Fokus liegt dabei nicht zuletzt auf konkreten Umsetzungsoptionen, die Airlock bietet, um schon heute die Brücke zwischen klassischer Identitätsprüfung und SSI-basierten Prozessen zu schlagen.

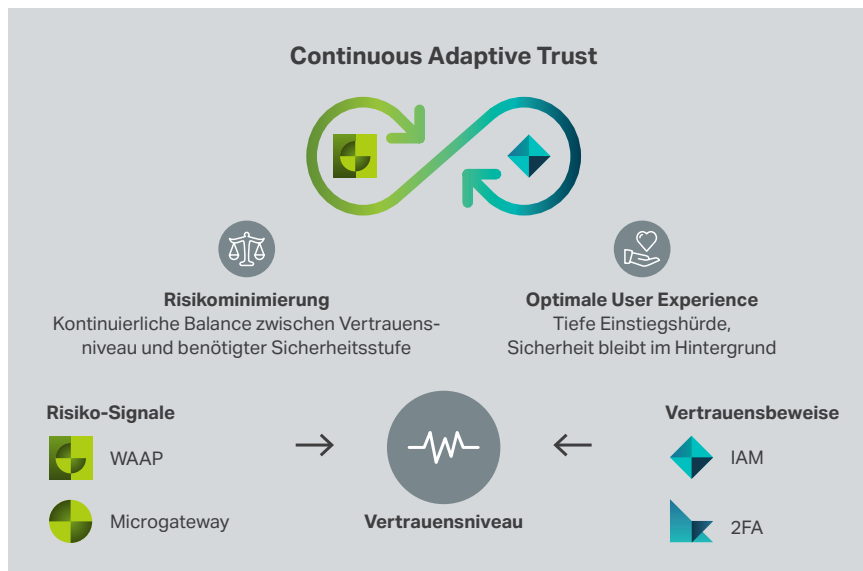
## Zusammenarbeit mit WAAP-Systemen

Web Application & API Protection (WAAP) und cIAM müssen sich immer mehr gegenseitig ergänzen. Identity Awareness innerhalb der Sicherheitsarchitektur ermöglicht es, Anomalien besser zu erkennen, Zugriff granular zu kontrollieren und Compliance zu stärken. Eine enge Integration von WAAP und cIAM trägt zu einer adaptiven Sicherheitsarchitektur bei.

### Airlock-Praxis

Durch die Kombination aus WAAP und cIAM von Airlock lässt sich das Prinzip von Continuous Adaptive Trust stichhaltig umsetzen. Unternehmen bietet dies die Möglichkeit, adaptive Sicherheitsmechanismen optimal in alle digitalen Prozesse zu integrieren. Über die Integration mit Bot-Detection, Anomaly Shield und risikobasierten Policies sind Airlock-Kunden nicht zuletzt in der Lage, alle Login-Versuche mithilfe von künstlicher Intelligenz und Machine Learning in Echtzeit zu analysieren, verdächtige Muster zu erkennen und schnell sowie adäquat zu reagieren – ohne dabei Kontrolle oder Compliance zu verlieren.





Quelle: Airlock

Die Bühler Group, deren Schwerpunkt im Bereich der mechanischen und thermischen Verfahrenstechnik liegt, setzt im Bereich Angriffserkennung gezielt auf das Zusammenspiel von WAAP und cIAM. Über vorgelagerte Authentisierung und dynamisches Whitelist-Filtering werden Webapplikationen vor unautorisiertem Zugriff geschützt. Dabei analysiert Airlock Gateway den gesamten Traffic zwischen Nutzern und Services. Angriffsversuche werden blockiert, noch bevor Hacker auf interne Systeme zugreifen können. Zusätzlichen Schutz bietet dabei das Airlock Anomaly Shield, das mittels Machine Learning auch unbekannte Angriffsarten und unerwünschte Bots erkennt. Auf diese Weise wurde der Schutz der Applikationen mit minimalem Aufwand deutlich erhöht – bei gleich hohem Datendurchsatz und ohne Einschränkungen für die Nutzer.

## Identity Federation und hybride Landschaften

Grosse Unternehmen arbeiten oft mit einer Vielzahl von Identitätsquellen. cIAM-Systeme sollten föderierte Identitäten nahtlos unterstützen – egal ob über Partner, soziale Netzwerke oder staatliche E-ID-Systeme. Die Fähigkeit, mehrere Trust-Frameworks gleichzeitig zu bedienen, ist ein zentraler Erfolgsfaktor.

### Airlock-Praxis

Hier bietet Airlock Unternehmen grösstmögliche Flexibilität. In dem Zusammenhang gilt FIDO2 als erste Wahl für starke Authentifizierung, wobei gerade in hybriden Szenarien mit klassischen MFA-Methoden kombiniert werden sollte. Airlock unterstützt eine umfassende FIDO2-Integration – inklusive fallbasierter Entscheidung, wann FIDO verpflichtend zum Einsatz kommt oder Fallback-basiert ergänzt wird.

[Raiffeisen Schweiz](#) – der Zusammenschluss aller Schweizer Raiffeisenbanken – setzt seit Jahren auf die benutzerfreundlichen und flexiblen Authentifizierungslösungen von Airlock. Ziel war eine zentrale Sicherheitsinfrastruktur mit einer Authentifizierungsplattform, die Kunden via Single Sign-On einfachen Zugang zu allen Services bietet und den nahtlosen Wechsel zwischen digitalen Applikationen ohne Neu anmeldung ermöglicht – ausser bei Anwendungen mit höheren Identifikations- und Sicherheitsanforderungen. Das integrierte IAM-System stellt Administratoren die nötigen Werkzeuge zur Verfügung, um Zugriffsrechte gezielt und effizient zu steuern. Die Lösung ist auf externe Nutzer ausgerichtet und für eine grosse Zahl digitaler Identitäten konzipiert. Die Kombination aus vorgelagerter WAF, IAM und zentraler Authentifizierungsplattform nimmt Angreifern effektiv den Wind aus den Segeln und überzeugt durch Detailtiefe: Je nach Applikation lassen sich unterschiedliche Authentifizierungsstärken definieren, was eine optimale Balance zwischen Compliance, Nutzereinwilligung, IT-Sicherheit und Nutzererlebnis schafft.

### **Nähe zum Kunden und digitale Souveränität**

Die Wahl eines clAM-Systems sollte auch strategische Überlegungen einbeziehen: Welche Kontrollmöglichkeiten bestehen über Datenflüsse? Gibt es Hersteller-Support in der eigenen Jurisdiktion? Wer kontrolliert Updates, Wartung und Innovationszyklen? Wie steht es um die Datenschutzrisiken im Hinblick auf Cloud-First-Anbieter? Digitale Souveränität ist nicht nur für Behörden, sondern auch für regulierte Branchen ein kritisches Auswahlkriterium.

### **Airlock-Praxis**

Die Authentifizierungslösungen von Airlock zeichnen sich nicht nur durch ihre Sicherheit, Effizienz und Nutzerfreundlichkeit aus. Der Kunde hat zudem stets die Wahl zwischen On-Prem-Installationen oder einer Umsetzung in der Cloud im Software-as-a-Service-Modell.

Wie erfolgreich ein IT-Security-Projekt ist, hängt entscheidend davon ab, wie passgenau die Lösung auf die Anforderungen des Auftraggebers abgestimmt ist. Hier überzeugte Airlock in der Zusammenarbeit mit den deutschen [Wasserstraßen- und Schifffahrtsämtern \(WSÄ\)](#) – als Unterbehörden der Wasserstraßen- und Schifffahrtsverwaltung des Bundes (WSV) – auf ganzer Linie. Aufgrund der fortschreitenden Digitalisierung der Seefahrt galt es im Projekt insbesondere, den exponentiell ansteigenden Sicherheitsvorgaben gerecht zu werden. Gefragt war eine ganzheitliche Lösung zur Absicherung der vermehrt browserbasierten Webanwendungen, die allen Partnern des maritimen Marktes eine gemeinsame Prozessbearbeitung ermöglicht. Die Absicherung der sensiblen Webanwendungen erfolgte über die vorgeschaltete WAAP-Lösung von Airlock, ausgewählt aufgrund ihrer hohen Verfügbarkeit und ihres modularen Aufbaus. Airlock Gateway kann jederzeit mit neuen Anforderungen mitwachsen, egal ob IAM, 2FA oder IT-Container. Damit stellt sich die WSV zukunftsicher auf. Von Erstkontakt bis zum Go-Live verlief das Projekt reibungslos. Das Team von Airlock überzeugte durch sein Verständnis für die spezifischen Bedürfnisse und den sehr guten Support. Das Projekt konnte on-time und in-budget umgesetzt werden – was im Behördenumfeld keineswegs selbstverständlich ist.

# 4. Airlock: Puzzlen mit Methode

Airlock bietet eine skalierbare Plattform, die alle wesentlichen Sicherheitsmechanismen abdeckt und sich nahtlos in bestehende IT-Infrastrukturen integrieren lässt – unabhängig davon, ob es sich um On-Premises-Umgebungen, hybride Architekturen oder reine Cloud-Installationen handelt. Durch die Unterstützung von containerisierten Anwendungen und Cloud-Integrationen ist die Lösung optimal auf zukünftige Technologien vorbereitet. Auch in der post-quantenfähigen Ära bietet Airlock bereits heute die Grundlagen, um langfristig sichere Authentifizierungsprozesse zu gewährleisten.



## Aufbau und Struktur der Sicherheitsarchitektur

Die Architektur von Airlock basiert auf einem mehrschichtigen Sicherheitsmodell:

- ▶ **1. Web Application Firewall (WAF):**
  - Schutz vor OWASP Top 10 Bedrohungen (z.B. SQL Injection, Cross-Site Scripting)
  - Schutzmechanismen gegen DDoS-Angriffe und Bots
  
- ▶ **2. API Security:**
  - Sicherer Zugriff auf API durch Authentifizierung und Autorisierung
  - Schutz von Datenströmen durch Verschlüsselung und Zugriffskontrollen
  
- ▶ **3. Identity and Access Management (IAM):**
  - Verwaltung von Benutzeridentitäten und Zugriffsrechten
  - Starke Authentifizierung: Multi-Faktor (MFA), Single Sign-On (SSO) und passwortlose Verfahren
  
- ▶ **4. Anomaly Shield:**
  - Erkennung von Anomalien im Nutzerverhalten
  - Echtzeit-Überwachung und automatische Reaktion auf Bedrohungen

▶ **5. Microservices und Container-Umgebungen:**

- Nahtlose Integration in Kubernetes-Cluster
- Schutz verteilter Service-Architekturen

▶ **6. Cloud-Integrationen:**

- Unterstützung für AWS, Azure und Google Cloud ohne Vendor Lock-in
- Konsistente Sicherheitsrichtlinien über alle Umgebungen hinweg
- Im SaaS-Modell verfügbar, reversible Migration zwischen Cloud und On-Prem

▶ **7. 2FA:**

- Auswahl zwischen vielfältigen Authentifizierungsmethoden (One-Touch, Offline QR-Code, Passcode und Passwordless)
- Nahtlose Integration in moderne Single Page Applications (SPA) und native Smartphone Apps

Die modulare Architektur erlaubt es, neue Sicherheitsmechanismen schnell zu etablieren und Anpassungen flexibel umzusetzen. So bleibt die Sicherheitsarchitektur stets auf dem neuesten Stand der Technik und schützt Anwendungen zuverlässig vor aktuellen Bedrohungen.

Über flexible Flows, Benutzersegmentierung und ein fein steuerbares Risiko-Scoring lässt sich auf Basis der Airlock-Lösungen ein Sicherheitsmodell etablieren, das sich dynamisch anpasst und Anwenderfreundlichkeit ins Zentrum stellt. Unternehmen können so stufenweise auf neue Verfahren umsteigen, regulatorische Anforderungen erfüllen und das Nutzererlebnis konsequent verbessern.

# 5. Fazit

Moderne Authentifizierung ist zur strategischen Kernaufgabe geworden – und sie stellt höhere Anforderungen als je zuvor. Die Komplexität beim sicheren Umgang mit digitalen Identitäten nimmt konsequent zu, gleichzeitig wird der Aspekt der Benutzerfreundlichkeit zunehmend wichtiger, insbesondere im Zuge der Wettbewerbsfähigkeit. Denn wer Kunden nicht die Experience liefern kann, die sie erwarten, verliert.

Vor diesem Hintergrund rückt die Leistungsfähigkeit des eingesetzten cIAM-Systems immer stärker in den Fokus: Dieses bildet das Rückgrat moderner Authentifizierung und bei der Auswahl einer geeigneten Lösung sollte neben maximaler Offenheit gegenüber gegenwärtigen und zukünftigen Standards insbesondere auf Modularität und Adaptivität sowie den Aspekt der Datenhoheit in Abwägung von On-Prem- und Cloud-Ansätzen geachtet werden. Zukunftsfähigkeit ist das entscheidende Stichwort und so sind Unternehmen gut damit beraten, bestehende Strukturen auf Herz und Nieren zu prüfen: Inwieweit halten die eigenen Prozesse aktuellen und zukünftigen Anforderungen Stand? Wo ergeben sich neue Chancen, wo verbergen sich Risiken? Und wie steht es um den Aspekt der digitalen Souveränität?

Es zählt eine stabile cIAM-Plattform, die schon heute Standards wie FIDO2, OAuth2 und SAML umsetzt und zudem Wege in Richtung SSI und Post-Quantum-Kryptografie eröffnet. Dass sich die Investition in ein modernes cIAM-System sowohl aus IT- als auch aus Business-Perspektive lohnt, steht ausser Frage. Laut aktueller Studien rentiert sich die Einführung innerhalb kürzester Zeit. Unternehmen profitieren nicht nur von hoher Effizienz im Zuge schnellerer Entwicklungszyklen, verkürzter Time-to-Market und geringeren Ausfallzeiten. Auch Support-Kosten lassen sich über den Einsatz von Self-Service-Funktionen und passwortlosen Verfahren deutlich senken. Und last but not least darf der Einfluss auf Conversion Rates keinesfalls vergessen werden. Schliesslich geht von optimierten Login-Flows und passwortloser Authentifizierung ein nachweislich positiver Effekt auf Abschlussraten in Onboarding-Prozessen aus.

Entscheidend ist es, die einzelnen Prioritäten entlang der spezifischen Ausgangslage und Zielstellung zu identifizieren und umzusetzen. Das stimmige Zusammenfügen der relevanten Funktionsbausteine ist ein kontinuierlicher Prozess, in dem die Stärken von Airlock voll und ganz zum Tragen kommen. Im Auftrag der Kunden setzt Airlock seit jeher alles daran, die Puzzleteile moderner Authentifizierung in ein individuell stimmiges Gesamtbild zu bringen.

# Glossar und Abkürzungen

<b>Begriff</b>	<b>Beschreibung</b>
<b>API</b>	Application Programming Interface – Schnittstelle zur Anwendungsprogrammierung
<b>CIAM</b>	Customer Identity and Access Management – Verwaltung von Identitäten und Zugriffen für Kunden
<b>Claim Mappings</b>	Mechanismus zur Zuordnung von Identitätsattributen (z.B. Rollen, Gruppen) beim Föderieren von Identitäten
<b>CRYSTALS-Kyber</b>	Post-Quantum-Verschlüsselungsalgorithmus auf Gitterbasis – Kandidat für PQC-Standards
<b>ECC</b>	Elliptic Curve Cryptography – Effizientes asymmetrisches Verschlüsselungsverfahren
<b>EUDI / E-ID</b>	European Digital Identity – Europäische Digitale Identität zur länderübergreifenden Nutzung
<b>ETSI</b>	European Telecommunications Standards Institute – Europäische Organisation für Telekommunikationsstandards
<b>Federation Layer</b>	Schicht in CIAM-Systemen, die unterschiedliche Identity-Provider integriert und föderierte Identitäten verwaltet
<b>FIDO</b>	Fast Identity Online – Authentifizierungsstandard für passwortlose Anmeldungen
<b>FIDO2</b>	Erweiterung des FIDO-Standards für Webanwendungen mit biometrischer Authentifizierung
<b>IAM</b>	Identity and Access Management – Verwaltung von Benutzern und Berechtigungen in einem Netzwerk
<b>IdP</b>	Identity Provider – System, das digitale Identitäten bereitstellt und authentifiziert
<b>Identity Federation</b>	Zusammenschluss mehrerer IdPs, um Nutzern den Zugriff auf Ressourcen über Vertrauensbeziehungen zu ermöglichen
<b>Least-Privilege-Prinzip</b>	Sicherheitsprinzip, nach dem ein Benutzer nur die minimal notwendigen Rechte erhält
<b>MIM</b>	Machine Identity Management – Verwaltung und Sicherung von Identitäten für Maschinen und Dienste
<b>MFA</b>	Multi-Faktor-Authentifizierung – Mehrschichtige Sicherheitsüberprüfung beim Login

<b>Begriff</b>	<b>Beschreibung</b>
<b>NHI</b>	Non-Human Identities – Digitale Identitäten für Maschinen, Services und Anwendungen
<b>NIST</b>	National Institute of Standards and Technology – US-Behörde für IT-Sicherheits- und Kryptografiestandards
<b>POS</b>	Point of Sale – Verkaufspunkt, oft mit physischen oder digitalen Kassensystemen verbunden
<b>PQC</b>	Post-Quanten-Kryptografie – Verschlüsselungsverfahren, die auch gegen Quantencomputer sicher sind
<b>RPA-Bot</b>	Robotic Process Automation Bot – Software-Roboter zur Automatisierung von Geschäftsprozessen
<b>RSA</b>	Kryptografischer Algorithmus zur asymmetrischen Verschlüsselung – basiert auf der Faktorisierung grosser Zahlen
<b>SSI</b>	Self-Sovereign Identity – Selbstbestimmte digitale Identität ohne zentrale Kontrolle
<b>SSO</b>	Single Sign-On – Einmalige Authentifizierung für den Zugriff auf mehrere Anwendungen
<b>TLS</b>	Transport Layer Security – Protokoll zur sicheren Datenübertragung im Internet
<b>Token</b>	Digitaler Nachweis für Authentifizierung oder Autorisierung – z.B. JWT oder OAuth-Token
<b>Trust-Policy / Trust-Brokering</b>	Regelwerk zur Bewertung von Identitätsquellen und Authentifizierungsverfahren in föderierten Umgebungen
<b>Vaults</b>	Sichere Speicherorte für geheime Informationen wie Passwörter, Keys oder Secrets
<b>Verifiable Credential</b>	Digitaler, kryptografisch signierter Identitätsnachweis in SSI-Ökosystemen
<b>WAF</b>	Web Application Firewall – Schutz vor Cyberangriffen auf Webanwendungen
<b>WAAP</b>	Web Application and API Protection – Integrierte Sicherheitsplattform zum Schutz von Webdiensten und APIs

## Weiterführende Ressourcen

Für weiterführende Informationen und vertiefende Einblicke in die behandelten Themen empfehlen wir folgende Ressourcen:

**FIDO Alliance:** [FIDO Alliance Webseite](#) – Offizielle Seite mit technischen Spezifikationen und Best Practices.

**European Digital Identity (EUDI):** [Europäische Kommission](#) – Digitale Identität – Informationen zur Europäischen Digitalen Identität.

**Post-Quanten-Kryptografie:** [NIST Post-Quantum Cryptography Project](#) – Informationen zu quantensicheren Verschlüsselungen.

**OWASP Top 10:** [OWASP Foundation](#) – Übersicht der zehn grössten Sicherheitsrisiken für Webanwendungen.

**Airlock Secure Access Hub:** [Airlock Webseite](#) – Informationen zur Plattform und deren Integrationsmöglichkeiten.

### **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 [airlock.com](http://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 über 400 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  
8032 Zürich  
+41 44 268 89 00  
[info@airlock.com](mailto:info@airlock.com)

[airlock.com](http://airlock.com)

**ergon**

Copyright © 2025 Ergon Informatik AG. All Rights Reserved. All technical documentation that is made available by Ergon Informatik AG is the copyrighted work of Ergon Informatik AG and is owned by Ergon Informatik AG. Ergon, the Ergon logo, «smart people – smart software» and Airlock are registered trademarks of Ergon Informatik AG. Microsoft and ActiveDirectory are registered trademarks or trademarks of Microsoft Corporation in the United States and /or other countries. Other products or trademarks mentioned are the property of their respective owners.