



AI, Security-Zonen und digitale Fragmentierung: Wie eine identitätszentrierte Architektur sichere Entscheidungsräume schafft



Detlev Altendorf
Account und Partner
Manager



AI ist in aller Munde

- Smartphones
- Spiele
- Bildbearbeitung
- Rüstung
- ChatGPT
- Autonomes Fahren
- Das Allheilmittel für alles?

Was Unternehmen beim Umgang mit generativen KI-Anwendungen beachten sollten:

- 1. Datenschutz
- 2. Datenqualität
- 3. Geistiges Eigentum
- 4. Transparenz
- 5. Haftung und Risikomanagement
- 6. Menschliche Überprüfung
- 7. Mitarbeitende schulen
- 8. Ethische Überlegungen
- 9. Coding
- 10. Plugins
- Quelle: <https://www.dihk.de/de/themen-und-positionen/wirtschaft-digital/digitalisierung/was-unternehmen-beim-umgang-mit-generativen-ki-anwendungen-beachten-sollten-94832>



Deutsche
Industrie- und Handelskammer

Anwendungsfälle für künstliche Intelligenz in Unternehmen

KI bei der Arbeit

9 KI-Anwendungen in der Industrie

1. Kundenerfahrung, Service und Support
2. Gezieltes Marketing
3. Intelligenter Lieferketten
4. Intelligenter Prozesse
5. Sicherere Prozesse
6. Qualitätskontrolle und Qualitätssicherung
7. Kontextbezogenes Verständnis
8. Optimierung
9. Effektiveres Lernen



Beispiele für die branchenspezifische Verwendung von KI



GESUNDHEITSWESEN

KI wird eingesetzt, um riesige Mengen von Patientendaten zu analysieren und Muster und Erkenntnisse aufzudecken, die Menschen allein nicht finden können. Andere intelligente Tools helfen Ärzten bei der Entwicklung individueller Behandlungspläne für Patienten.



FINANZDIENSTLEISTUNGEN

KI wird bei der Betrugs-erkennung eingesetzt, um nahezu sofortige Entscheidungen zu treffen. KI wird auch für die Vermögensverwaltung, Kreditgenehmigungen und Handelsentscheidungen sowie für andere Finanzdienstleistungen verwendet.



INDUSTRIELLE WARTUNG

KI wird zur Überwachung und Vorhersage von Wartungsarbeiten für Maschinen genutzt. KI wird auch in Fabriken eingesetzt, um die Effizienz zu steigern.



TRANSPORTWESEN

KI ermöglicht selbstfahrende Fahrzeuge, die mit zunehmender Navigationserfahrung immer intelligenter werden. Sie werden auch eingesetzt, um das Verkehrsmanagement und die Transportlogistik zu optimieren.

ILLUSTRATION: LEMONG/GETTY IMAGES, MSTYLE/ADOBE STOCK

©2021 TECHTARGET. ALL RIGHTS RESERVED. TechTarget

– Quelle: <https://www.computerweekly.com/de/tipp/9-Anwendungen-von-kuenstlicher-Intelligenz-in-der-Industrie>

ComputerWeekly.de

AIRLOCK®



ergon

Founded 1984

440 employees

85% with University Degree

Swiss made software

SWISS
ARBEIT
GEBER
AWARD

2021



AIRLOCK

20 years experience

**650 Airlock customers
in over 30 countries**

**> 30'000 protected
applications**

**Very high customer
satisfaction**

Sales bei Ergon Informatik:

- ERP
- Mail
- File-Server
- JIRA
- SharePoint
- CRM
- Confluence

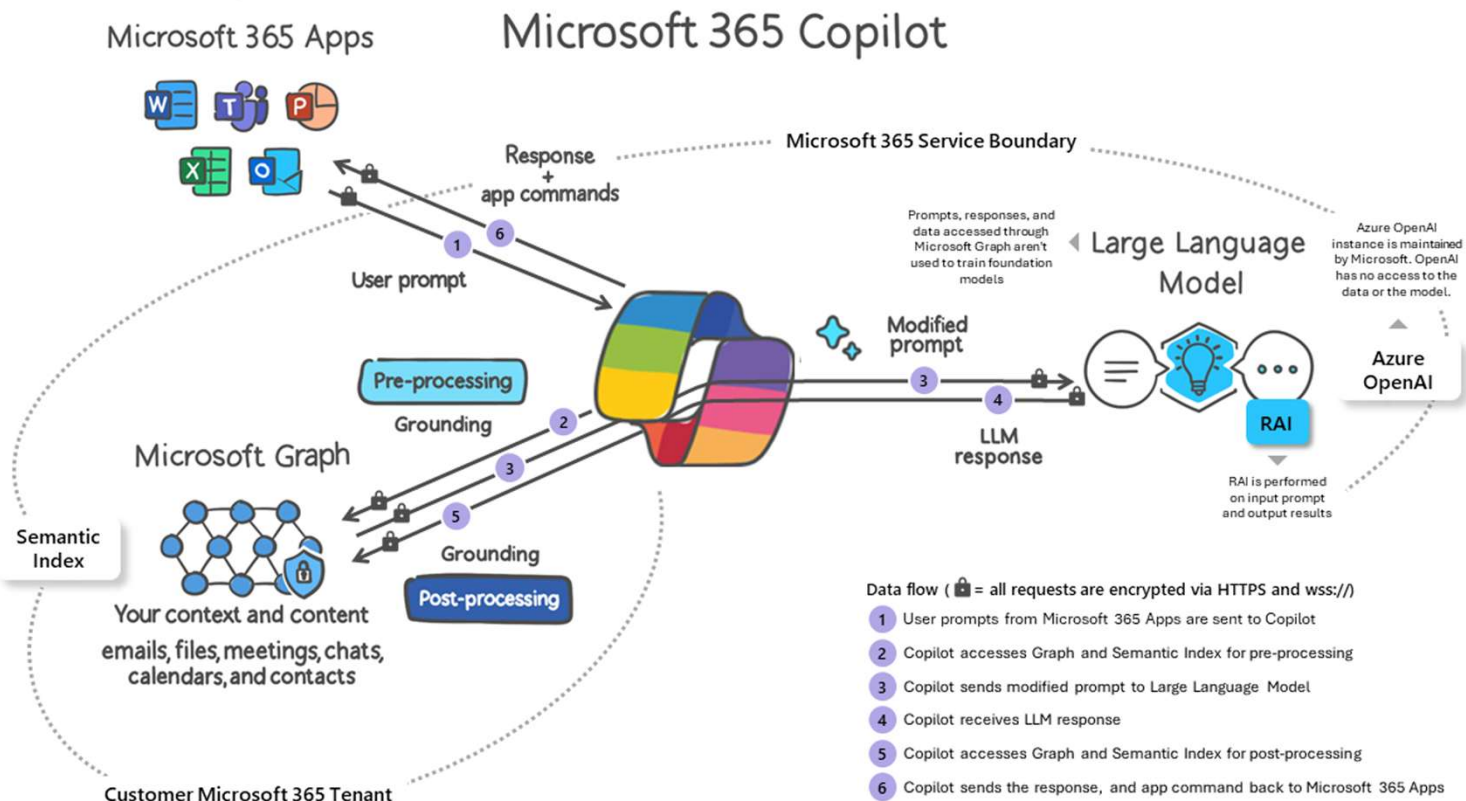




Unsere Kunden und Interessenten:

- Internationale Unternehmen
- Standorte in Europa, USA, Japan & China (z.B. Pharma)
- AI-Driven Automation
- Investment Protection
- Security
- AI Resultate abhängig von Datenqualität:
 - Quellen im WWW
 - Fake News
 - Alternative Facts
 - Intranet (> 1000 Quellen)

Wie kann ich der Datenflut Herr werden?



Quelle: www.microsoft.com

AI gestützte Kommunikation

User

User Experience
UI customization
Self-Services
Social Logins

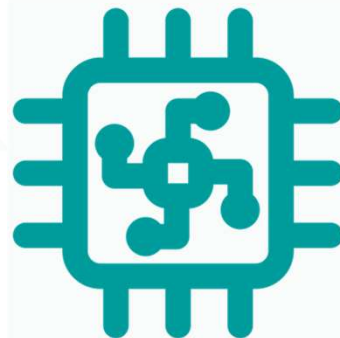


Legal and Compliance

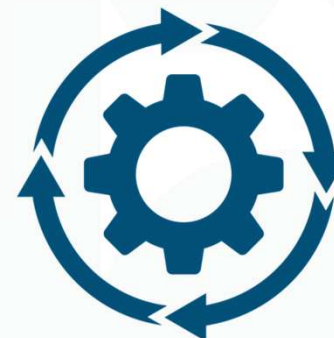
GDPR und DSGVO
SCA (PSD2)
Transaction Approval
Cooldown Period



FIDO / Passkey
Bring your own Authentication
Risk-based Authentication



Technology

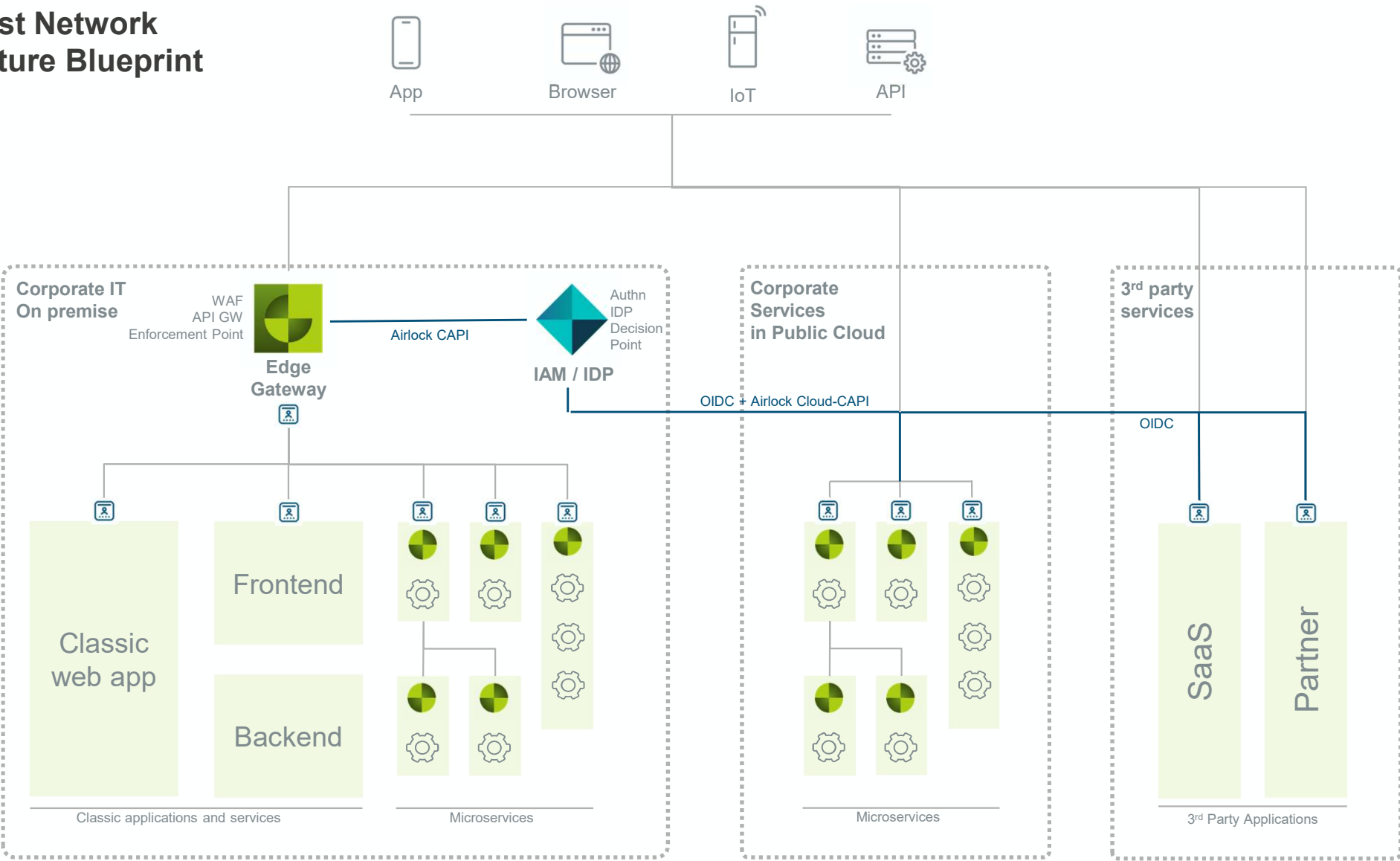


Operation

7*24 Availability
Cost efficiency
Performance

AIRLOCK®

Zero Trust Network Architecture Blueprint



 Edge Gateway  Microgateway  IAM / IDP  Identity Token (e.g. JWT)

Modern business solutions use identities from different sources



Sources of identities:

- Partners and Suppliers
- Merger und Acquisitions
- Social Login
- Pressure of Hyperscalers

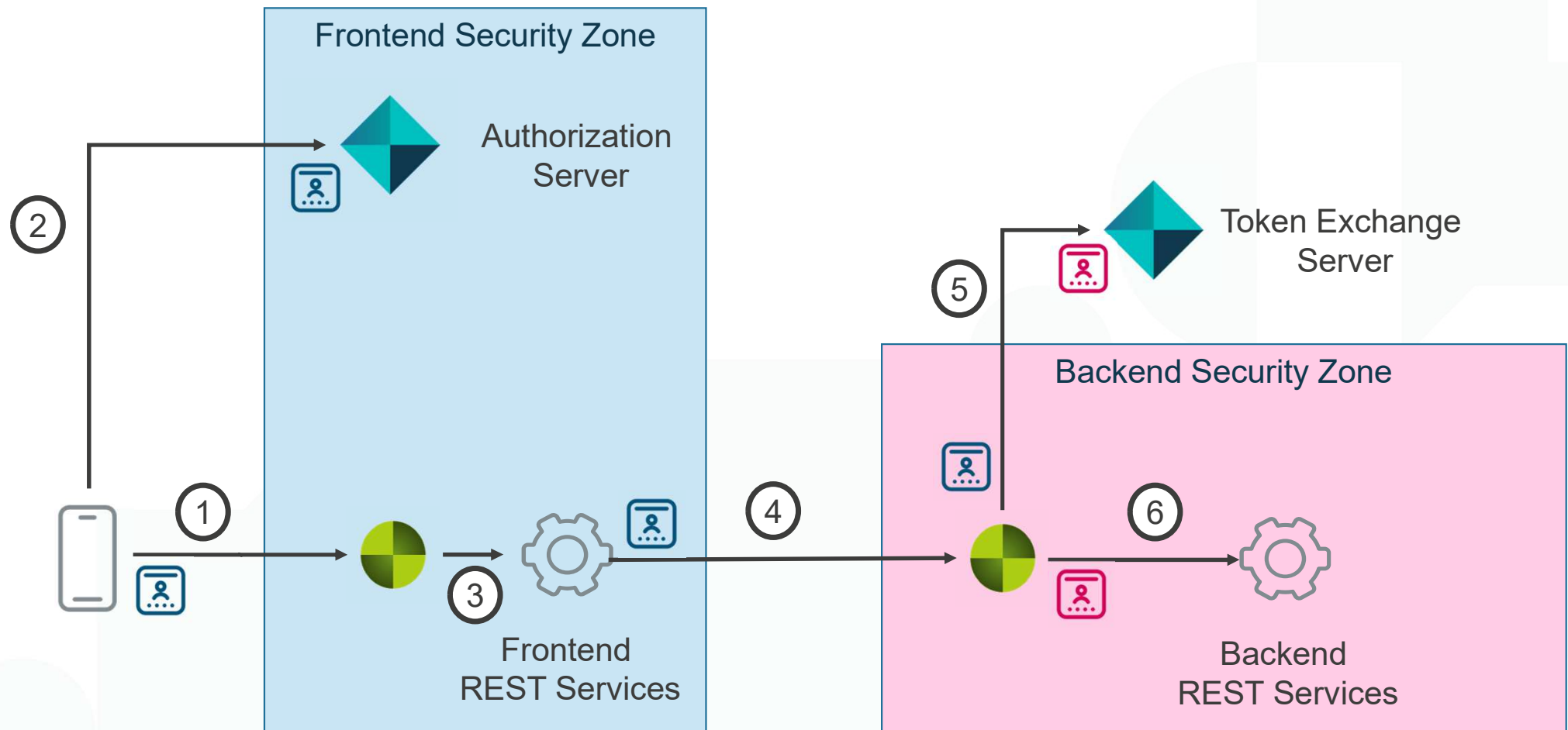
Goal: SSO for End Users with
Identity Federation



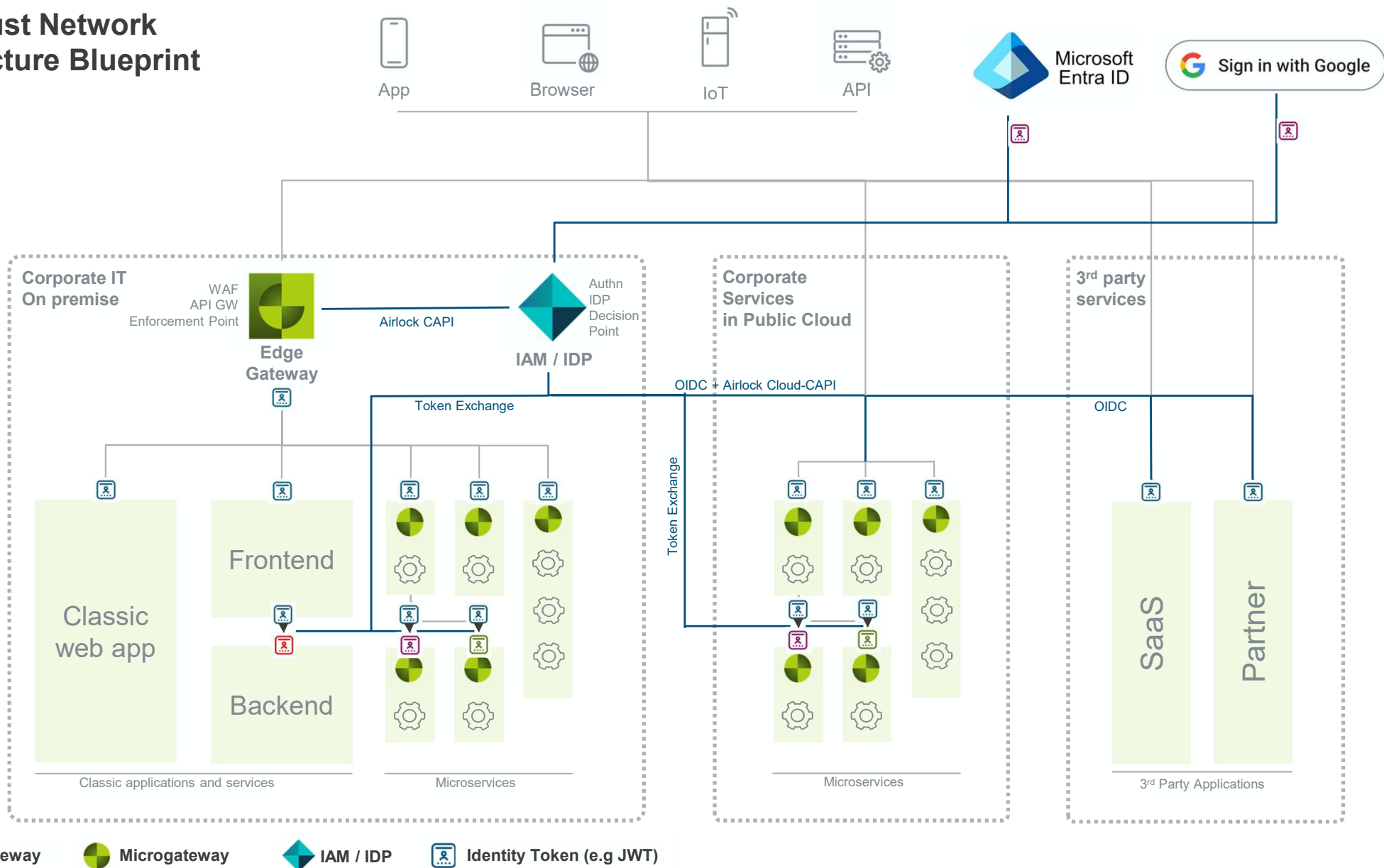
AI gestützte Kommunikation

- MS Copilot
- Power Apps
- Maschine zu Maschine Kommunikation
- Multiple IDPs: Entra ID, cIAM im Intranet, SAP, China
 - Unterschiedliche Tokens!
- Wie ist das technisch machbar?

Token Exchange (RFC 8693) – internal Use Case



Zero Trust Network Architecture Blueprint





Conclusions

Modern Protocols like OAuth, OpenID Connect and Token Exchange allow us to manage identities in hybrid cloud setups

Policy enforcement covers both security filtering and identity enforcement and therefore meets the ZTNA paradigm

Implementation in the infrastructure layer reduces costs, complexity and time to market

Applications remain unchanged and unaware of the additional security measures in place



Detlev Altendorf
Partner & Account Manager Deutschland

detlev.altendorf@airlock.com
M +49 151 2063 4413

