# Identity Management in Microsoft Infrastrukturen

## Single Sign-on für die Hybrid Cloud

**Begriffe wie Zero Trust Network Access (ZTNA), Identity and Access Management (IAM) und Identity Provider (IdP) sind in aller Munde, aber was verbirgt sich dahinter? Sollen Cloud Services etabliert werden, tauchen diese Begriffe ebenso auf wie der Wunsch nach Single Sign-on (SSO). Die Dienste und Ressourcen, welche es mit einzubinden gilt, reichen von Cloud-Diensten wie Salesforce oder Microsoft Azure bis hin zu On-Premises-Servern wie einem Cisco Unified Communications Manager. Dabei kommen unterschiedliche Protokolle wie WS-Federation, SAMLv2, OAuth 2.0 oder OpenID Connect zum Einsatz. Häufig stehen sie zudem vor der Herausforderung, dass ein lokales Microsoft Active Directory angebunden werden muss. Der Kurs verschafft einen Überblick über die Authentisierungsmöglichkeiten in einer hybriden Umgebung, beschreibt die Funktionsweise der unterschiedlichen SSO-Protokolle, erläutert aus welchen Komponenten eine IAM-Infrastruktur besteht, und wie eine On-Premise-Infrastruktur mit einer Cloud-Architektur verschmelzen kann. Das Training liefert zudem einen umfassenden Überblick über den Aufbau einer IAM-Lösung am Beispiel einer Microsoft-Infrastruktur.**

### Kursinhalt

- Authentisierungs-Varianten
- Review: Zertifikate und Digitale Signaturen
- Funktionsweise von Single Sign-on (SSO)
- Protokolle: Kerberos, SAMLv2, OAuth 2.0, OpenID Connect
- Unterschiede zwischen Active Directory und dem Azure AD
- Microsoft Entra (Azure AD, Permissions Management, Verified ID)
- Authentisierung in einer hybriden Infrastruktur (Password sync., Pass-Through, Modern Authentication)
- Authentisierung und Provisionierung (SCIM) in einer hybriden Infrastruktur
- Hinzufügen einer Multi-Factor Authentication (MFA)
- Device Registration Service
- Aufbau einer ADFS Infrastruktur
- Privileged Access Management und Privileged Identity Management

E-Book Sie erhalten das ausführliche deutschsprachige Unterlagenpaket von ExperTeach – Print, E-Book und personalisiertes PDF! Bei Online-Teilnahme erhalten Sie das E-Book sowie das personalisierte PDF.

### Zielgruppe

Der Kurs richtet sich an Solution Engineers, welche ihre lokale IT-Infrastruktur mit Diensten aus der Cloud sicher koppeln wollen.

### Voraussetzungen

Die Teilnehmer sollten Vorkenntnisse im Bereich Benutzerverwaltung, Authentisierung und Autorisierung aufweisen können. Der Kurs Active Directory Fundamentals & LDAP – Protokolle, Architektur und Funktionsweise ist eine gute Basis. Des weiteren sollten Sie über Kenntnisse im Bereich von X.509 Zertifikaten verfügen. Diese erlangen Teilnehmer im Rahmen des Kurses Zertifikate & PKI Training – Verschlüsselung, Authentisierung & Integrität.

### Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/**IDMA**

### Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

### Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

### Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

| Training | Preise zzgl. MwSt. |
|---|---|
| **Termine in Deutschland** | **2 TageCHF 1.975,-** |
| **Online Training** | **2 TageCHF 1.975,-** |

| Termin/Kursort | | Kurssprache Deutsch | |
|---|---|---|---|
| 17.06.-18.06.24 | HY Frankfurt | 14.10.-15.10.24 | HY Frankfurt |
| 17.06.-18.06.24 | HY Online | 14.10.-15.10.24 | HY Online |

Stand 17.04.2024

# Inhaltsverzeichnis

## Identity Management in Microsoft Infrastrukturen – Single Sign-on für die Hybrid Cloud


**1 Single Sign-on**
1.1 Authentisierungs-Methoden
1.1.1 Challenge/Response
1.1.2 Transport Layer Security
1.1.3 Mutual Authentication
1.1.4 Zwischenspeicherung von Anmeldeinformationen
1.2 Kerberos
1.3 Claim-based Authentication
1.3.1 Zugriff auf die Ressource
1.3.2 Authentifizierung
1.3.3 Erzeugung des Tokens
1.3.4 Zustellung des Tokens
1.3.5 Authentisierung gegenüber der Ressource
1.3.6 Austausch der Metadaten
1.3.7 Cookie
1.3.8 Erneute Authentisierung
1.3.9 Zugriff auf weiteren Dienst
1.4 Kerberos Integration
1.5 Business to Business

**2 Protokolle**
2.1 Kerberos
2.2 WS-Federation & WS-Trust
2.3 Security Assertion Markup Language (SAML)
2.3.1 Komponenten von SAML
2.3.2 Ablauf einer SAML-Authentication
2.4 Open Authentication 2 (OAuth2)
2.4.1 Beispiel
2.4.2 Authorization Code
2.4.3 Implicit Grant
2.4.4 Resource Owner Password Credentials
2.4.5 Client Credentials
2.4.6 Auswahl des Flows
2.4.7 OAuth als Service Provider (Client) nutzen
2.5 OpenID Connect
2.6 Entwicklungsumgebung

**3 Infrastruktur**
3.1 Active Directory
3.1.1 Lokale Infrastruktur
3.1.2 Azure AD
3.1.3 Unterschiede: AD – Azure AD
3.1.4 Azure AD Domain Services
3.2 Microsoft Entra
3.2.1 Azure Active Directory
3.2.2 Permissions Management
3.2.3 Verified ID
3.3 Hybride Umgebungen
3.3.1 Authentisierung
3.3.2 Modern Authentication
3.3.3 Azure als zusätzlichen IdP nutzen
3.3.4 Provisionierung
3.3.5 System for Cross-Domain Identity Management
3.4 Multi-Factor Authentication
3.4.1 Microsoft Authenticator
3.4.2 Conditional Access & Web Application Proxy
3.4.3 Azure AD MFA-Server
3.5 Device Registration Service
3.6 Identity Provider Infrastruktur
3.6.1 Identity Provider (IdP)
3.6.2 Relying Party (RP)
3.6.3 Metadata
3.6.4 Token
3.6.5 Zertifikate
3.6.6 Authentisierung
3.6.7 Reverse Proxy
3.6.8 Hochverfügbarkeit
3.6.9 Anbieter
3.7 PIM & PAM
3.7.1 Tier Konzept
3.7.2 Privileged Access Management
3.7.3 Privileged Identity Management



**ExperTeach AG**
Kronenstrasse 11 · 8735 St. Gallenkappel · Telefon: +41 55 420 2591 · Fax: +41 55 420 2592 · info@experteach.ch · www.experteach.ch