

Identitäts- und Berechtigungsmanagement

Maximilian Heim¹

¹Hochschule Albstadt-Sigmaringen

IT-GRC Seminar, Juni 2024

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance

- Unterschiedliche Definitionen

¹Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

- Unterschiedliche Definitionen
- Identitätsmanagement: Digitale Identität

¹Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

- Unterschiedliche Definitionen
- Identitätsmanagement: Digitale Identität
- Digitale Identität: Bezeichner, Zugangsdaten und Attribute¹

¹Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

- Unterschiedliche Definitionen
- Identitätsmanagement: Digitale Identität
- Digitale Identität: Bezeichner, Zugangsdaten und Attribute¹
- Wichtig: Digitale Identitäten sind nicht nur Personen

¹Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

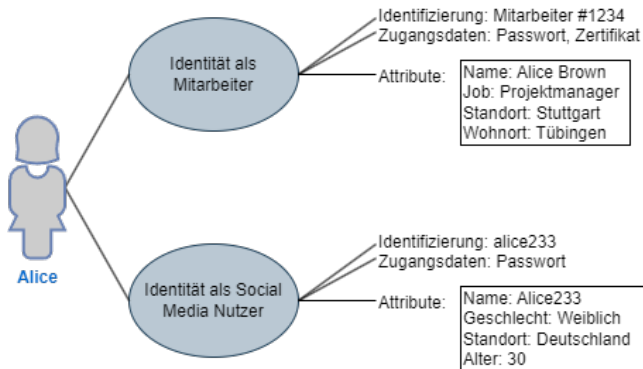


Abbildung: Digitale Identität - Basierend auf Grafik 2.1 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

- Management von digitalen Identitäten

- Management von digitalen Identitäten
- Aufgabenbereiche: Umfangreich

- Management von digitalen Identitäten
- Aufgabenbereiche: Umfangreich
- Grundlegender Prozess: Identitätslebenszyklus

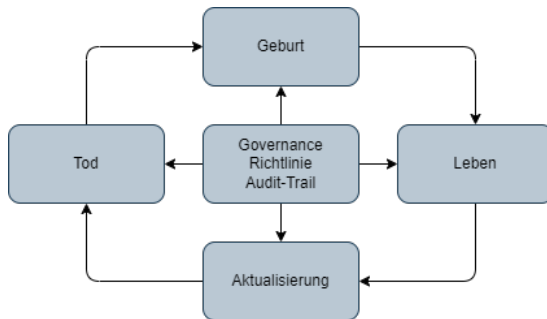


Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

- Geburt:
Datensammlung
und Validierung,
Zugangsdaten

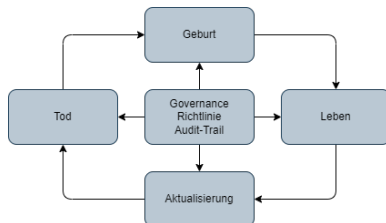
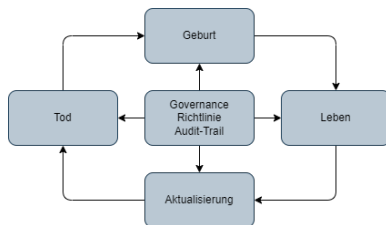


Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi



- Geburt: Datensammlung und Validierung, Zugangsdaten
- Leben: Authentifizierung, Weitergabe

Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

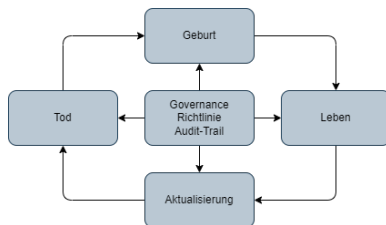


Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

- Geburt: Datensammlung und Validierung, Zugangsdaten
- Leben: Authentifizierung, Weitergabe
- Änderung: Änderungen, Zugangsdaten

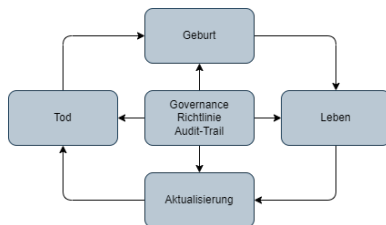


Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

- Geburt: Datensammlung und Validierung, Zugangsdaten
- Leben: Authentifizierung, Weitergabe
- Änderung: Änderungen, Zugangsdaten
- Tod: Kündigung, Löschung

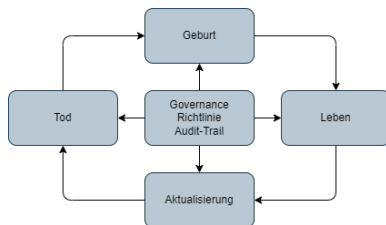


Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

- Geburt: Datensammlung und Validierung, Zugangsdaten
- Leben: Authentifizierung, Weitergabe
- Änderung: Änderungen, Zugangsdaten
- Tod: Kündigung, Löschung
- Governance: Richtlinien, Audit-Trail

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- **Berechtigungsmanagement**
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance

- Kombination aus Ressource und Operation²

²Alexander Tolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017. ISBN: 978-3-658-17987-8.

- Kombination aus Ressource und Operation²
- Beispiele:

²Alexander Tolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017. ISBN: 978-3-658-17987-8.

- Kombination aus Ressource und Operation²
- Beispiele:
 - Wer darf Inhalte des \\ad.hochschule.de Verzeichnisses ändern?

²Alexander Tolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017. ISBN: 978-3-658-17987-8.

- Kombination aus Ressource und Operation²
- Beispiele:
 - Wer darf Inhalte des \\ad.hochschule.de Verzeichnisses ändern?
 - Wer darf in Azure DevOps Repositories löschen?

²Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017. ISBN: 978-3-658-17987-8.

- Kombination aus Ressource und Operation²
- Beispiele:
 - Wer darf Inhalte des \\ad.hochschule.de Verzeichnisses ändern?
 - Wer darf in Azure DevOps Repositories löschen?
 - Wer darf in AWS Zertifikate erstellen?

²Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017. ISBN: 978-3-658-17987-8.

- Kombination aus Ressource und Operation²
- Beispiele:
 - Wer darf Inhalte des \\ad.hochschule.de Verzeichnisses ändern?
 - Wer darf in Azure DevOps Repositories löschen?
 - Wer darf in AWS Zertifikate erstellen?
 - Wer darf das Wohnheim in der Poststraße 22 betreten?

²Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017. ISBN: 978-3-658-17987-8.

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Aufgaben:

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Aufgaben:
 - Wie werden Berechtigungen unterteilt? (Berechtigungskonzept - RBAC, ABAC, Kombination)

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Aufgaben:
 - Wie werden Berechtigungen unterteilt? (Berechtigungskonzept - RBAC, ABAC, Kombination)
 - Wie werden Berechtigungen vergeben und entzogen, wie werden irreguläre Berechtigungen vergeben?

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Aufgaben:
 - Wie werden Berechtigungen unterteilt? (Berechtigungskonzept - RBAC, ABAC, Kombination)
 - Wie werden Berechtigungen vergeben und entzogen, wie werden irreguläre Berechtigungen vergeben?
 - Wie werden Berechtigungskontrollen technisch umgesetzt? (Authorisierung)

- Identitäts- und Berechtigungsmanagement = Identity access management (IAM)

- Identitäts- und Berechtigungsmanagement = Identity access management (IAM)
- Unterscheidung: IAM vs CIAM

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance

Identitäts- und Berechtigungsmanagement-Systeme

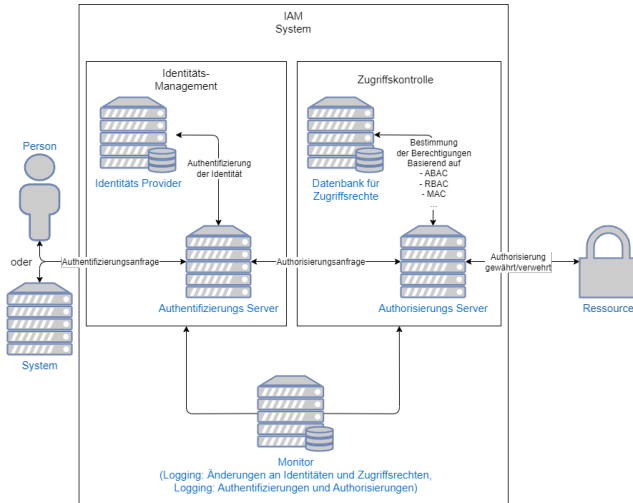


Abbildung: IAM System - Basierend auf Grafik 1 aus „Identity and access management using distributed ledger technology: A survey“ von Fariba Ghaffari, Komal Gilani, Emmanuel Bertin und Noel Crespi

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance

- CIO: Planung und Leitung der benötigten IT-Systeme

- CIO: Planung und Leitung der benötigten IT-Systeme
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzstandards und Sicherheitsstandards, Awareness Trainings, interne Audits...

- CIO: Planung und Leitung der benötigten IT-Systeme
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzstandards und Sicherheitsstandards, Awareness Trainings, interne Audits...
- IT-Betrieb: Implementierung und Wartung der involvierten Technik

- CIO: Planung und Leitung der benötigten IT-Systeme
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzstandards und Sicherheitsstandards, Awareness Trainings, interne Audits...
- IT-Betrieb: Implementierung und Wartung der involvierten Technik
- Personalabteilung: Identity-Lifecycle Management

- CIO: Planung und Leitung der benötigten IT-Systeme
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzstandards und Sicherheitsstandards, Awareness Trainings, interne Audits...
- IT-Betrieb: Implementierung und Wartung der involvierten Technik
- Personalabteilung: Identity-Lifecycle Management
- Helpdesk: Hilfe bei Authentifizierung und Authorisierung

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
 - Cloud (IDaaS - Identity as a Service) vs. On Premise

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
 - Cloud (IDaaS - Identity as a Service) vs. On Premise
 - Prozesse: Automatisiertes Lifecycle Management, Risikoanalyse, Audit

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
 - Cloud (IDaaS - Identity as a Service) vs. On Premise
 - Prozesse: Automatisiertes Lifecycle Management, Risikoanalyse, Audit
 - Technologie: Multi Faktor Authentifizierung, Single Sign On

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
 - Cloud (IDaaS - Identity as a Service) vs. On Premise
 - Prozesse: Automatisiertes Lifecycle Management, Risikoanalyse, Audit
 - Technologie: Multi Faktor Authentifizierung, Single Sign On
 - Integration: Active Directory, Microsoft Office, AWS, HR Anwendungen

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
 - Cloud (IDaaS - Identity as a Service) vs. On Premise
 - Prozesse: Automatisiertes Lifecycle Management, Risikoanalyse, Audit
 - Technologie: Multi Faktor Authentifizierung, Single Sign On
 - Integration: Active Directory, Microsoft Office, AWS, HR Anwendungen
 - ...

Technische Aspekte

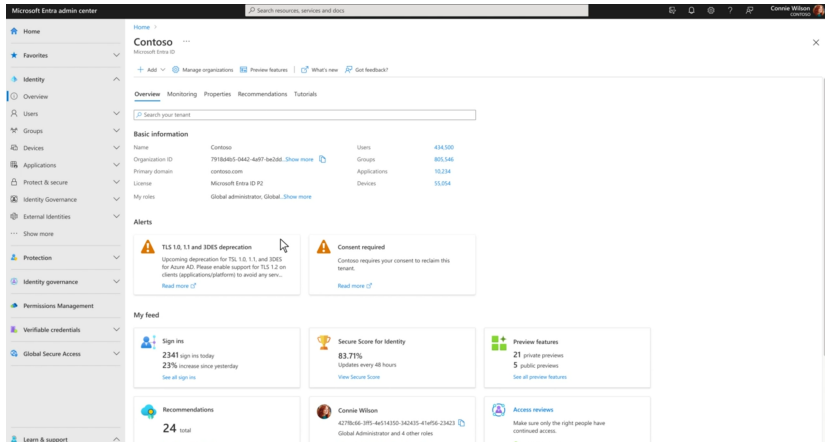


Abbildung: Microsoft Entra ID - von

<https://www.microsoft.com/de-de/security/business/microsoft-entra>

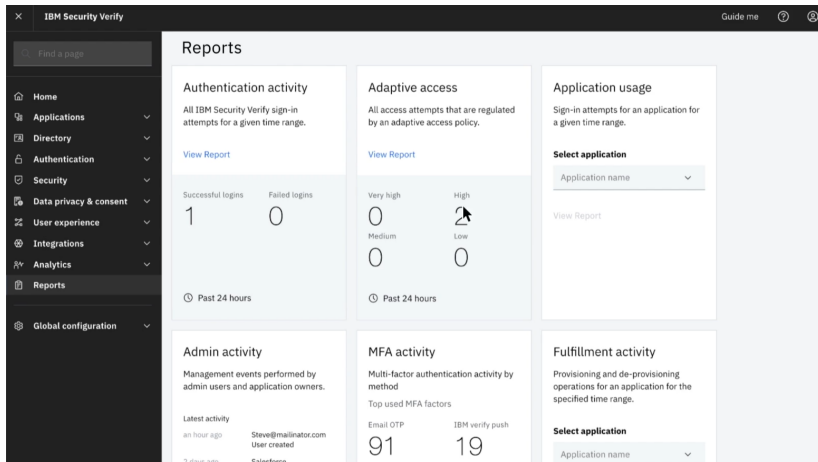


Abbildung: IBM Security Verify - von <https://www.ibm.com/de-de/products/verify-saas>

Technische Aspekte

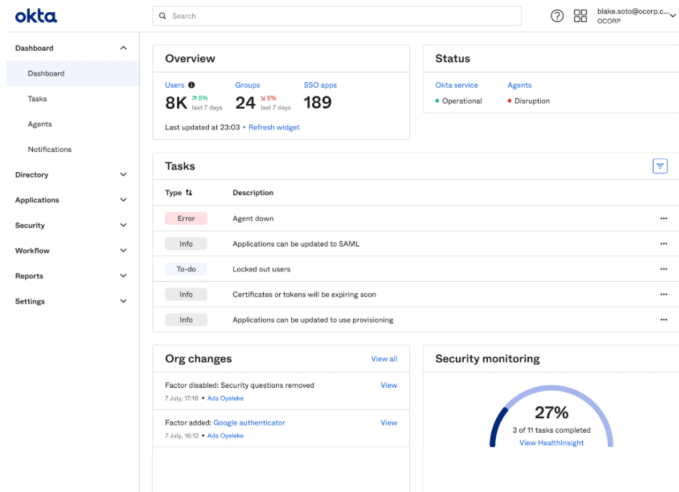


Abbildung: Okta Workforce Identity Cloud - von <https://thectoclub.com/tools/best-identity-and-access-management-solutions/>

- ISO 27001: Annex A.9 definiert Zugangssteuerung

- ISO 27001: Annex A.9 definiert Zugangssteuerung
- IT-Grundschutz: BSI-Standard 200-1, ORP.4

- ISO 27001: Annex A.9 definiert Zugangssteuerung
- IT-Grundschutz: BSI-Standard 200-1, ORP.4
- NIST 800-53A: Kapitel Access Control Family (AC) und Identification and Authentication Family (IA)

- ISO 27001: Annex A.9 definiert Zugangssteuerung
- IT-Grundschutz: BSI-Standard 200-1, ORP.4
- NIST 800-53A: Kapitel Access Control Family (AC) und Identification and Authentication Family (IA)
- ...

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance

- EuroSOX: Berechtigungskontrolle, Funktionstrennung

- EuroSOX: Berechtigungskontrolle, Funktionstrennung
- KonTraG: Risikomanagementsystem

- EuroSOX: Berechtigungskontrolle, Funktionstrennung
- KonTraG: Risikomanagementsystem
- GoBD: Berechtigungskontrollen, Nachvollziehbarkeit von Änderungen

- EuroSOX: Berechtigungskontrolle, Funktionstrennung
- KonTraG: Risikomanagementsystem
- GoBD: Berechtigungskontrollen, Nachvollziehbarkeit von Änderungen
- EU-DSGVO und BDSG: Speicherung, Verarbeitung und Weitergabe von personenbezogenen Daten

- EuroSOX: Berechtigungskontrolle, Funktionstrennung
- KonTraG: Risikomanagementsystem
- GoBD: Berechtigungskontrollen, Nachvollziehbarkeit von Änderungen
- EU-DSGVO und BDSG: Speicherung, Verarbeitung und Weitergabe von personenbezogenen Daten
- ...

- Vielen dank für eure Aufmerksamkeit!

- Vielen dank für eure Aufmerksamkeit!
- Fragen?

- [1] Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.
- [2] Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017. ISBN: 978-3-658-17987-8.