

Identitäts- und Berechtigungsmanagement

Maximilian Heim¹

¹Hochschule Albstadt-Sigmaringen

IT-GRC Seminar, 19. Juni 2024

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance Aspekte

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance Aspekte

- Unterschiedliche Definitionen

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

- Unterschiedliche Definitionen
- Identitätsmanagement: Digitale Identität

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

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

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

- Unterschiedliche Definitionen
- Identitätsmanagement: Digitale Identität
- Digitale Identität: Bezeichner, Zugangsdaten und Attribute
- Wichtig: Digitale Identitäten sind nicht nur Personen¹

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

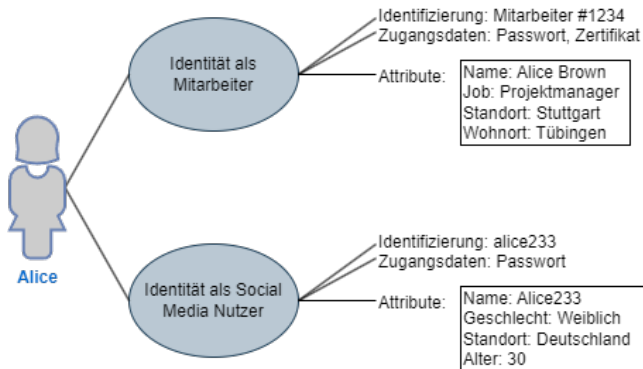


Abbildung: Digitale Identität - Basierend auf Grafik 2.1 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

- Management von digitalen Identitäten

² Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

³ Daniel Conta. "Leitfaden eines mandantenunabhängigen Identity Access Management". Diss. Hochschule für angewandte Wissenschaften Hamburg, 2017.

⁴ Sanket Devlekar und Vidyavati Ramteke. "Identity and access management: High-level conceptual framework". In: *Cardiometry* 24 (2022), S. 393–399.

- Management von digitalen Identitäten
- Gründe:

² Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

³ Daniel Conta. "Leitfaden eines mandantenunabhängigen Identity Access Management". Diss. Hochschule für angewandte Wissenschaften Hamburg, 2017.

⁴ Sanket Devlekar und Vidyavati Ramteke. "Identity and access management: High-level conceptual framework". In: *Cardiometry* 24 (2022), S. 393–399.

- Management von digitalen Identitäten
- Gründe:
 - Speicherung, Nutzung und Weitergabe von Identitätsinformationen

²Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

³Daniel Conta. "Leitfaden eines mandantenunabhängigen Identity Access Management". Diss. Hochschule für angewandte Wissenschaften Hamburg, 2017.

⁴Sanket Devlekar und Vidyavati Ramteke. "Identity and access management: High-level conceptual framework". In: *Cardiometry* 24 (2022), S. 393–399.

- Management von digitalen Identitäten
- Gründe:
 - Speicherung, Nutzung und Weitergabe von Identitätsinformationen
 - Berechtigungsmanagement

² Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

³ Daniel Conta. "Leitfaden eines mandantenunabhängigen Identity Access Management". Diss. Hochschule für angewandte Wissenschaften Hamburg, 2017.

⁴ Sanket Devlekar und Vidyavati Ramteke. "Identity and access management: High-level conceptual framework". In: *Cardiometry* 24 (2022), S. 393–399.

- Management von digitalen Identitäten
- Gründe:
 - Speicherung, Nutzung und Weitergabe von Identitätsinformationen
 - Berechtigungsmanagement
- Aufgabenbereiche:

² Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

³ Daniel Conta. "Leitfaden eines mandantenunabhängigen Identity Access Management". Diss. Hochschule für angewandte Wissenschaften Hamburg, 2017.

⁴ Sanket Devlekar und Vidyavati Ramteke. "Identity and access management: High-level conceptual framework". In: *Cardiometry* 24 (2022), S. 393–399.

- Management von digitalen Identitäten
- Gründe:
 - Speicherung, Nutzung und Weitergabe von Identitätsinformationen
 - Berechtigungsmanagement
- Aufgabenbereiche:
 - Prozesse (Identitätslebenszyklus)

² Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

³ Daniel Conta. "Leitfaden eines mandantenunabhängigen Identity Access Management". Diss. Hochschule für angewandte Wissenschaften Hamburg, 2017.

⁴ Sanket Devlekar und Vidyavati Ramteke. "Identity and access management: High-level conceptual framework". In: *Cardiometry* 24 (2022), S. 393–399.

- Management von digitalen Identitäten
- Gründe:
 - Speicherung, Nutzung und Weitergabe von Identitätsinformationen
 - Berechtigungsmanagement
- Aufgabenbereiche:
 - Prozesse (Identitätslebenszyklus)
 - Technische Umsetzung (Speicherung, Weitergabe und Authentifizierung)²

²Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

³Daniel Conta. "Leitfaden eines mandantenunabhängigen Identity Access Management". Diss. Hochschule für angewandte Wissenschaften Hamburg, 2017.

⁴Sanket Devlekar und Vidyavati Ramteke. "Identity and access management: High-level conceptual framework". In: *Cardiometry* 24 (2022), S. 393–399.

- Management von digitalen Identitäten
- Gründe:
 - Speicherung, Nutzung und Weitergabe von Identitätsinformationen
 - Berechtigungsmanagement
- Aufgabenbereiche:
 - Prozesse (Identitätslebenszyklus)
 - Technische Umsetzung (Speicherung, Weitergabe und Authentifizierung)²
 - Compliance mit Gesetzen und Standards³

²Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

³Daniel Conta. "Leitfaden eines mandantenunabhängigen Identity Access Management". Diss. Hochschule für angewandte Wissenschaften Hamburg, 2017.

⁴Sanket Devlekar und Vidyavati Ramteke. "Identity and access management: High-level conceptual framework". In: *Cardiometry* 24 (2022), S. 393–399.

- Management von digitalen Identitäten
- Gründe:
 - Speicherung, Nutzung und Weitergabe von Identitätsinformationen
 - Berechtigungsmanagement
- Aufgabenbereiche:
 - Prozesse (Identitätslebenszyklus)
 - Technische Umsetzung (Speicherung, Weitergabe und Authentifizierung)²
 - Compliance mit Gesetzen und Standards³
 - Auditierung von Ist vs. Soll⁴

² Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

³ Daniel Conta. "Leitfaden eines mandantenunabhängigen Identity Access Management". Diss. Hochschule für angewandte Wissenschaften Hamburg, 2017.

⁴ Sanket Devlekar und Vidyavati Ramteke. "Identity and access management: High-level conceptual framework". In: *Cardiometry* 24 (2022), S. 393–399.

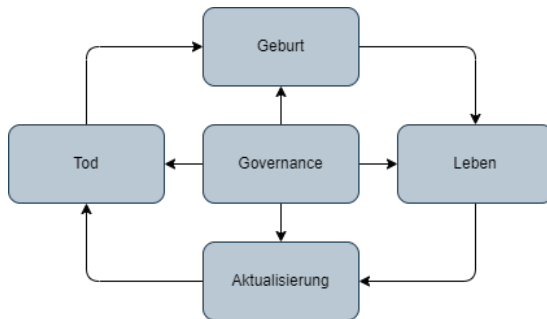
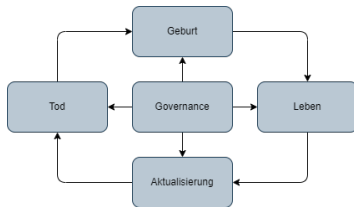


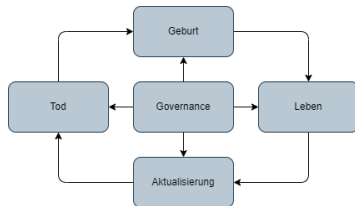
Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi



- 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

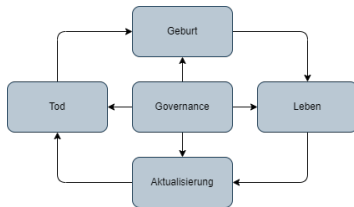
²Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.



- 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

²Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.



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

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

²Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

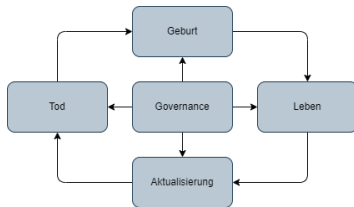


Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

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

²Elisa Bertino und Kenji Takahashi. *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

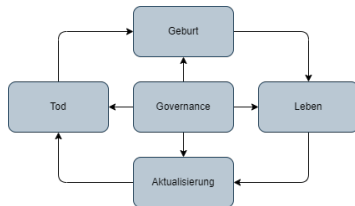


Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

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

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

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

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

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance Aspekte

- Kombination aus Ressource und Operation⁵

⁵ Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Kombination aus Ressource und Operation⁵
- Beispiele:

⁵ Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Kombination aus Ressource und Operation⁵
- Beispiele:
 - Wer darf Inhalte des \\ad.hochschule.de Verzeichnisses ändern?

⁵ Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Kombination aus Ressource und Operation⁵
- Beispiele:
 - Wer darf Inhalte des \\ad.hochschule.de Verzeichnisses ändern?
 - Wer darf in Azure DevOps Repositories löschen?

⁵ Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Kombination aus Ressource und Operation⁵
- Beispiele:
 - Wer darf Inhalte des \\ad.hochschule.de Verzeichnisses ändern?
 - Wer darf in Azure DevOps Repositories löschen?
 - Wer darf in AWS Zertifikate erstellen?

⁵ Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Kombination aus Ressource und Operation⁵
- 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?

⁵ Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

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

⁶BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. (Besucht am 28.05.2024).

⁷Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

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

⁶BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. (Besucht am 28.05.2024).

⁷Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe:
 - PoLP/Principle of Least Privilege⁶

⁶BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. (Besucht am 28.05.2024).

⁷Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe:
 - PoLP/Principle of Least Privilege⁶
 - SoD/Funktionstrennung

⁶BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. (Besucht am 28.05.2024).

⁷Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe:
 - PoLP/Principle of Least Privilege⁶
 - SoD/Funktionstrennung
 - Rückverfolgbarkeit

⁶BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. (Besucht am 28.05.2024).

⁷Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe:
 - PoLP/Principle of Least Privilege⁶
 - SoD/Funktionstrennung
 - Rückverfolgbarkeit
- Aufgaben:

⁶BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. (Besucht am 28.05.2024).

⁷Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe:
 - PoLP/Principle of Least Privilege⁶
 - SoD/Funktionstrennung
 - Rückverfolgbarkeit
- Aufgaben:
 - Berechtigungskonzept auf Unternehmen anpassen - RBAC, ABAC ...

⁶BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. (Besucht am 28.05.2024).

⁷Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe:
 - PoLP/Principle of Least Privilege⁶
 - SoD/Funktionstrennung
 - Rückverfolgbarkeit
- Aufgaben:
 - Berechtigungskonzept auf Unternehmen anpassen - RBAC, ABAC ...
 - Technische Umsetzung (Authorisierung)

⁶BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. (Besucht am 28.05.2024).

⁷Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe:
 - PoLP/Principle of Least Privilege⁶
 - SoD/Funktionstrennung
 - Rückverfolgbarkeit
- Aufgaben:
 - Berechtigungskonzept auf Unternehmen anpassen - RBAC, ABAC ...
 - Technische Umsetzung (Authorisierung)
 - Compliance mit Gesetzen und Standards

⁶BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. (Besucht am 28.05.2024).

⁷Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe:
 - PoLP/Principle of Least Privilege⁶
 - SoD/Funktionstrennung
 - Rückverfolgbarkeit
- Aufgaben:
 - Berechtigungskonzept auf Unternehmen anpassen - RBAC, ABAC ...
 - Technische Umsetzung (Authorisierung)
 - Compliance mit Gesetzen und Standards
 - Auditierung Ist vs. Soll⁷

⁶BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. (Besucht am 28.05.2024).

⁷Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance Aspekte

Identitäts- und Berechtigungsmanagement-Systeme

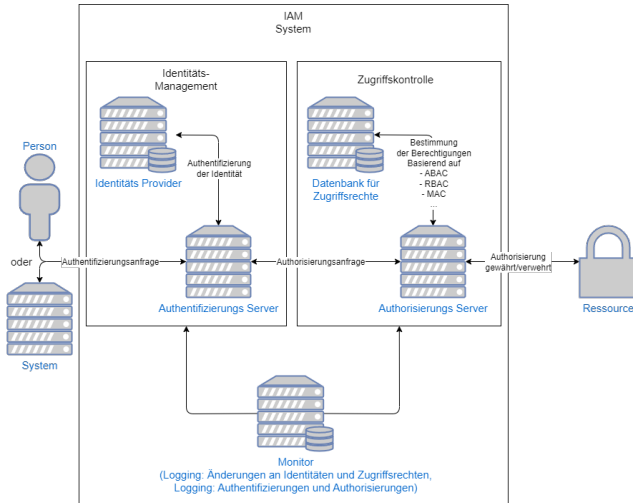


Abbildung: IAM System - Basierend auf Grafik 1 aus „Identity and access management using distributed ledger technology: A survey“ von Fariba Ghaffari, Komal Gilani, Emmanuel Bertin und Noel Crespi

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance Aspekte

- CIO: Verantwortlich für Prozesse und Technologien

⁸ Marco Casassa Mont u. a. "Economics of identity and access management: Providing decision support for investments". In: *2010 IEEE/IFIP Network Operations and Management Symposium Workshops*. IEEE. 2010, S. 134–141.

⁹ Microsoft. *Identity and Access Administrator Career Path*. 2024. (Besucht am 29.05.2024).

¹⁰ Ishaq Azhar Mohammed. "Systematic review of identity access management in information security". In: *International Journal of Innovations in Engineering Research and Technology* 4.7 (2017), S. 1–7.

¹¹ Mikko Ylen u. a. "Centralized password management in a global enterprise". *Magisterarb*. 2004.

- CIO: Verantwortlich für Prozesse und Technologien
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzgesetzen und Sicherheitsstandards, Awareness Trainings, interne Audits...⁸

⁸ Marco Casassa Mont u. a. "Economics of identity and access management: Providing decision support for investments". In: *2010 IEEE/IFIP Network Operations and Management Symposium Workshops*. IEEE. 2010, S. 134–141.

⁹ Microsoft. *Identity and Access Administrator Career Path*. 2024. (Besucht am 29.05.2024).

¹⁰ Ishaq Azhar Mohammed. "Systematic review of identity access management in information security". In: *International Journal of Innovations in Engineering Research and Technology* 4.7 (2017), S. 1–7.

¹¹ Mikko Ylen u. a. "Centralized password management in a global enterprise". *Magisterarb*. 2004.

- CIO: Verantwortlich für Prozesse und Technologien
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzgesetzen und Sicherheitsstandards, Awareness Trainings, interne Audits...⁸
- IT-Betrieb: Implementierung und Wartung der involvierten Technik⁹

⁸ Marco Casassa Mont u. a. "Economics of identity and access management: Providing decision support for investments". In: *2010 IEEE/IFIP Network Operations and Management Symposium Workshops*. IEEE. 2010, S. 134–141.

⁹ Microsoft. *Identity and Access Administrator Career Path*. 2024. (Besucht am 29.05.2024).

¹⁰ Ishaq Azhar Mohammed. "Systematic review of identity access management in information security". In: *International Journal of Innovations in Engineering Research and Technology* 4.7 (2017), S. 1–7.

¹¹ Mikko Ylen u. a. "Centralized password management in a global enterprise". *Magisterarb.* 2004.

- CIO: Verantwortlich für Prozesse und Technologien
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzgesetzen und Sicherheitsstandards, Awareness Trainings, interne Audits...⁸
- IT-Betrieb: Implementierung und Wartung der involvierten Technik⁹
- Personalabteilung: Identity-Lifecycle Management¹⁰

⁸ Marco Casassa Mont u. a. "Economics of identity and access management: Providing decision support for investments". In: *2010 IEEE/IFIP Network Operations and Management Symposium Workshops*. IEEE. 2010, S. 134–141.

⁹ Microsoft. *Identity and Access Administrator Career Path*. 2024. (Besucht am 29.05.2024).

¹⁰ Ishaq Azhar Mohammed. "Systematic review of identity access management in information security". In: *International Journal of Innovations in Engineering Research and Technology* 4.7 (2017), S. 1–7.

¹¹ Mikko Ylen u. a. "Centralized password management in a global enterprise". *Magisterarb*. 2004.

- CIO: Verantwortlich für Prozesse und Technologien
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzgesetzen und Sicherheitsstandards, Awareness Trainings, interne Audits...⁸
- IT-Betrieb: Implementierung und Wartung der involvierten Technik⁹
- Personalabteilung: Identity-Lifecycle Management¹⁰
- Helpdesk: Hilfe bei Authentifizierung und Authorisierung¹¹

⁸ Marco Casassa Mont u. a. "Economics of identity and access management: Providing decision support for investments". In: *2010 IEEE/IFIP Network Operations and Management Symposium Workshops*. IEEE. 2010, S. 134–141.

⁹ Microsoft. *Identity and Access Administrator Career Path*. 2024. (Besucht am 29.05.2024).

¹⁰ Ishaq Azhar Mohammed. "Systematic review of identity access management in information security". In: *International Journal of Innovations in Engineering Research and Technology* 4.7 (2017), S. 1–7.

¹¹ Mikko Ylen u. a. "Centralized password management in a global enterprise". *Magisterarb*. 2004.

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance Aspekte

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

¹²Michael Kunz u. a. "Analyzing Recent Trends in Enterprise Identity Management". In: *2014 25th International Workshop on Database and Expert Systems Applications*. 2014, S. 273–277.
DOI: [10.1109/DEXA.2014.62](https://doi.org/10.1109/DEXA.2014.62).

¹³IBM. *IBM Security Verify Access Management*. 2024. (Besucht am 28.05.2024).

¹⁴Okta. *Okta Integration Network* — Okta. 2024. (Besucht am 17.06.2024).

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
 - Neue Entwicklung: Cloud (IDaaS - Identity as a Service) im Gegensatz zu traditionellen On-Premise Lösungen¹²

¹²Michael Kunz u. a. "Analyzing Recent Trends in Enterprise Identity Management". In: *2014 25th International Workshop on Database and Expert Systems Applications*. 2014, S. 273–277. DOI: [10.1109/DEXA.2014.62](https://doi.org/10.1109/DEXA.2014.62).

¹³IBM. *IBM Security Verify Access Management*. 2024. (Besucht am 28.05.2024).

¹⁴Okta. *Okta Integration Network* — Okta. 2024. (Besucht am 17.06.2024).

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
 - Neue Entwicklung: Cloud (IDaaS - Identity as a Service) im Gegensatz zu traditionellen On-Premise Lösungen¹²
 - Implementieren Technologien für optimale Umsetzung: Multi Faktor Authentifizierung (OTP, Biometrie), Single Sign On. . .

¹²Michael Kunz u. a. "Analyzing Recent Trends in Enterprise Identity Management". In: *2014 25th International Workshop on Database and Expert Systems Applications*. 2014, S. 273-277. DOI: [10.1109/DEXA.2014.62](https://doi.org/10.1109/DEXA.2014.62).

¹³IBM. *IBM Security Verify Access Management*. 2024. (Besucht am 28.05.2024).

¹⁴Okta. *Okta Integration Network* — Okta. 2024. (Besucht am 17.06.2024).

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
 - Neue Entwicklung: Cloud (IDaaS - Identity as a Service) im Gegensatz zu traditionellen On-Premise Lösungen¹²
 - Implementieren Technologien für optimale Umsetzung: Multi Faktor Authentifizierung (OTP, Biometrie), Single Sign On. . .
 - Unterstützen Prozesse: Lifecycle Management, Risikoanalyse, Audit-Management¹³

¹²Michael Kunz u. a. "Analyzing Recent Trends in Enterprise Identity Management". In: *2014 25th International Workshop on Database and Expert Systems Applications*. 2014, S. 273-277. DOI: [10.1109/DEXA.2014.62](https://doi.org/10.1109/DEXA.2014.62).

¹³IBM. *IBM Security Verify Access Management*. 2024. (Besucht am 28.05.2024).

¹⁴Okta. *Okta Integration Network* — Okta. 2024. (Besucht am 17.06.2024).

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
 - Neue Entwicklung: Cloud (IDaaS - Identity as a Service) im Gegensatz zu traditionellen On-Premise Lösungen¹²
 - Implementieren Technologien für optimale Umsetzung: Multi Faktor Authentifizierung (OTP, Biometrie), Single Sign On. . .
 - Unterstützen Prozesse: Lifecycle Management, Risikoanalyse, Audit-Management¹³
 - Integration von Service Providern: Active Directory, Microsoft Office, AWS, HR Anwendungen¹⁴

¹²Michael Kunz u. a. "Analyzing Recent Trends in Enterprise Identity Management". In: *2014 25th International Workshop on Database and Expert Systems Applications*. 2014, S. 273-277. DOI: [10.1109/DEXA.2014.62](https://doi.org/10.1109/DEXA.2014.62).

¹³IBM. *IBM Security Verify Access Management*. 2024. (Besucht am 28.05.2024).

¹⁴Okta. *Okta Integration Network* — Okta. 2024. (Besucht am 17.06.2024).

Technische Aspekte

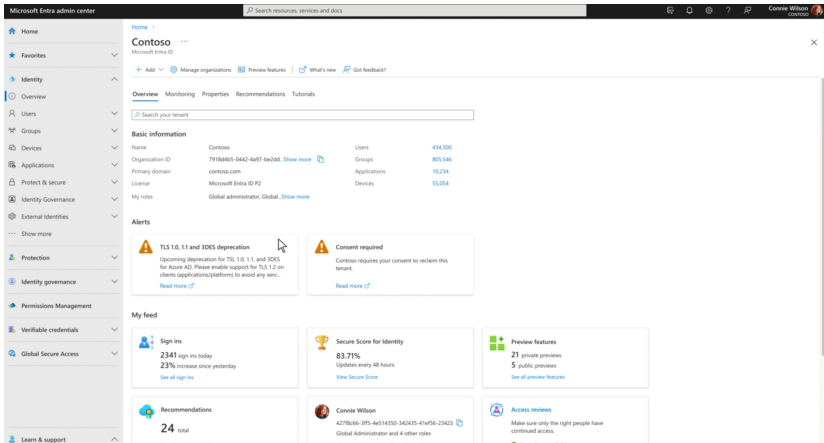


Abbildung: Microsoft Entra ID - von

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

Table of Contents

1 Identitätsmanagement- und Berechtigungsmanagement

- Identitätsmanagement
- Berechtigungsmanagement
- Identitäts- und Berechtigungsmanagement

2 Betriebliches Identitäts- und Berechtigungsmanagement

- Operative Aspekte
- Technische Aspekte
- Compliance Aspekte

- ISO/IEC 24760: Identitätsmanagement (Konzepte und operative Strukturen)¹⁵

¹⁵ISO. ISO/IEC 24760-1:2019(en) IT Security and Privacy - A framework for identity management - Part 1: Terminology and concepts. 2019. (Besucht am 28.05.2024).

¹⁶Heinrich Kersten u. a. "IT-Sicherheitsmanagement nach der neuen ISO 27001". In: *ISMS, Risiken, Kennziffern, Controls 2* (2020).

¹⁷BSI. BSI - BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS). Nov. 2017. (Besucht am 28.05.2024).

¹⁸BSI. ORP.4: Identitäts- und Berechtigungsmanagement. 2021. (Besucht am 28.05.2024).

- ISO/IEC 24760: Identitätsmanagement (Konzepte und operative Strukturen)¹⁵
- ISO 27001: Annex A.9 definiert Zugangssteuerung¹⁶

¹⁵ISO. ISO/IEC 24760-1:2019(en) IT Security and Privacy - A framework for identity management - Part 1: Terminology and concepts. 2019. (Besucht am 28.05.2024).

¹⁶Heinrich Kersten u. a. "IT-Sicherheitsmanagement nach der neuen ISO 27001". In: *ISMS, Risiken, Kennziffern, Controls 2* (2020).

¹⁷BSI. BSI - BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS). Nov. 2017. (Besucht am 28.05.2024).

¹⁸BSI. ORP.4: Identitäts- und Berechtigungsmanagement. 2021. (Besucht am 28.05.2024).

- ISO/IEC 24760: Identitätsmanagement (Konzepte und operative Strukturen)¹⁵
- ISO 27001: Annex A.9 definiert Zugangssteuerung¹⁶
- IT-Grundschutz: BSI-Standard 200-1, ORP.4: Identitäts- und Berechtigungsmanagement¹⁷¹⁸

¹⁵ISO. ISO/IEC 24760-1:2019(en) IT Security and Privacy - A framework for identity management - Part 1: Terminology and concepts. 2019. (Besucht am 28.05.2024).

¹⁶Heinrich Kersten u. a. "IT-Sicherheitsmanagement nach der neuen ISO 27001". In: *ISMS, Risiken, Kennziffern, Controls 2* (2020).

¹⁷BSI. BSI - BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS). Nov. 2017. (Besucht am 28.05.2024).

¹⁸BSI. ORP.4: Identitäts- und Berechtigungsmanagement. 2021. (Besucht am 28.05.2024).

- EuroSOX (EU-Richtlinie 2006/43/EG): Berechtigungskontrolle, Funktionstrennung

¹⁹ Daniel Conta. "Leitfaden eines mandantenunabhängigen Identity Access Management". Diss. Hochschule für angewandte Wissenschaften Hamburg, 2017.

²⁰ EU. VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES. Mai 2016. (Besucht am 28.05.2024).

²¹ Andrew Hindle. *Impact of GDPR on identity and Access Management*. März 2020.

- EuroSOX (EU-Richtlinie 2006/43/EG): Berechtigungskontrolle, Funktionstrennung
- KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich): Risikomanagementsystem

¹⁹ Daniel Conta. "Leitfaden eines mandantenunabhängigen Identity Access Management". Diss. Hochschule für angewandte Wissenschaften Hamburg, 2017.

²⁰ EU. VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES. Mai 2016. (Besucht am 28.05.2024).

²¹ Andrew Hindle. *Impact of GDPR on identity and Access Management*. März 2020.

- EuroSOX (EU-Richtlinie 2006/43/EG): Berechtigungskontrolle, Funktionstrennung
- KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich): Risikomanagementsystem
- GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff): Berechtigungskontrolle, Nachvollziehbarkeit von Änderungen

¹⁹ Daniel Conta. "Leitfaden eines mandantenunabhängigen Identity Access Management". Diss. Hochschule für angewandte Wissenschaften Hamburg, 2017.

²⁰ EU. VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES. Mai 2016. (Besucht am 28.05.2024).

²¹ Andrew Hindle. *Impact of GDPR on identity and Access Management*. März 2020.

- EuroSOX (EU-Richtlinie 2006/43/EG): Berechtigungskontrolle, Funktionstrennung
- KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich): Risikomanagementsystem
- GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff): Berechtigungskontrolle, Nachvollziehbarkeit von Änderungen
- EU-DSGVO (EU- Datenschutzgrundverordnung) und BDSG (Bundesdatenschutzgesetz): Speicherung, Verarbeitung und Weitergabe von personenbezogenen Daten¹⁹²⁰²¹

¹⁹ Daniel Conta. "Leitfaden eines mandantenunabhängigen Identity Access Management". Diss. Hochschule für angewandte Wissenschaften Hamburg, 2017.

²⁰ EU. VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES. Mai 2016. (Besucht am 28.05.2024).

²¹ Andrew Hindle. *Impact of GDPR on identity and Access Management*. März 2020.

- 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] BSI. *BSI - BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)*. Nov. 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.html (besucht am 28.05.2024).
- [3] BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium_Einzel_PDFs_2021/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2021.pdf?__blob=publicationFile&v=2 (besucht am 28.05.2024).

- [4] Daniel Conta. “Leitfaden eines mandantenunabhängigen Identity Access Management”. Diss. Hochschule für angewandte Wissenschaften Hamburg, 2017.
- [5] Sanket Devlekar und Vidyavati Ramteke. “Identity and access management: High-level conceptual framework”. In: *Cardiometry* 24 (2022), S. 393–399.
- [6] EU. VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES. Mai 2016. URL: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE> (besucht am 28.05.2024).
- [7] Andrew Hindle. *Impact of GDPR on identity and Access Management*. März 2020.

- [8] IBM. *IBM Security Verify Access Management*. 2024. URL: <https://www.ibm.com/products/verify-saas> (besucht am 28.05.2024).
- [9] ISO. *ISO/IEC 24760-1:2019(en) IT Security and Privacy - A framework for identity management - Part 1: Terminology and concepts*. 2019. URL: <https://www.iso.org/obp/ui/en/#iso:std:77582:en> (besucht am 28.05.2024).
- [10] Heinrich Kersten u. a. "IT-Sicherheitsmanagement nach der neuen ISO 27001". In: *ISMS, Risiken, Kennziffern, Controls 2* (2020).
- [11] Michael Kunz u. a. "Analyzing Recent Trends in Enterprise Identity Management". In: *2014 25th International Workshop on Database and Expert Systems Applications*. 2014, S. 273–277. DOI: 10.1109/DEXA.2014.62.

- [12] Microsoft. *Identity and Access Administrator Career Path*. 2024. URL: <https://learn.microsoft.com/en-us/plans/m14ntm3n2gy41q#> (besucht am 29.05.2024).
- [13] Ishaq Azhar Mohammed. "Systematic review of identity access management in information security". In: *International Journal of Innovations in Engineering Research and Technology* 4.7 (2017), S. 1–7.
- [14] Marco Casassa Mont u. a. "Economics of identity and access management: Providing decision support for investments". In: *2010 IEEE/IFIP Network Operations and Management Symposium Workshops*. IEEE. 2010, S. 134–141.
- [15] Okta. *Okta Integration Network — Okta*. 2024. URL: <https://www.okta.com/de/integrations/> (besucht am 17.06.2024).

- [16] Alexander Tsolkas und Klaus Schmidt. "Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen". In: Wiesbaden: Springer Fachmedien Wiesbaden, 2017.
- [17] Mikko Ylen u. a. "Centralized password management in a global enterprise". Magisterarb. 2004.