Identitäts- und Berechtigungsmanagement

Maximilian Heim[1]

[1]Hochschule Albstadt-Sigmaringen

IT-GRC Seminar, Juni 2024

Gliederung

Table of Contents

Identität im Kontext des Identitätsmanagements

- Unterschiedliche Definitionen

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

Identität im Kontext des Identitätsmanagements

- Unterschiedliche Definitionen
- Identitätsmanagement: Digitale Identität

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

Identität im Kontext des Identitätsmanagements

- Unterschiedliche Definitionen
- Identitätsmanagement: Digitale Identität
- Digitale Identität: Bezeichner, Zugangsdaten und Attribute[1]

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

Identität im Kontext des Identitätsmanagements

- Unterschiedliche Definitionen
- Identitätsmanagement: Digitale Identität
- Digitale Identität: Bezeichner, Zugangsdaten und Attribute[1]
- Wichtig: Digitale Identitäten sind nicht nur Personen

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

Digitale Identität

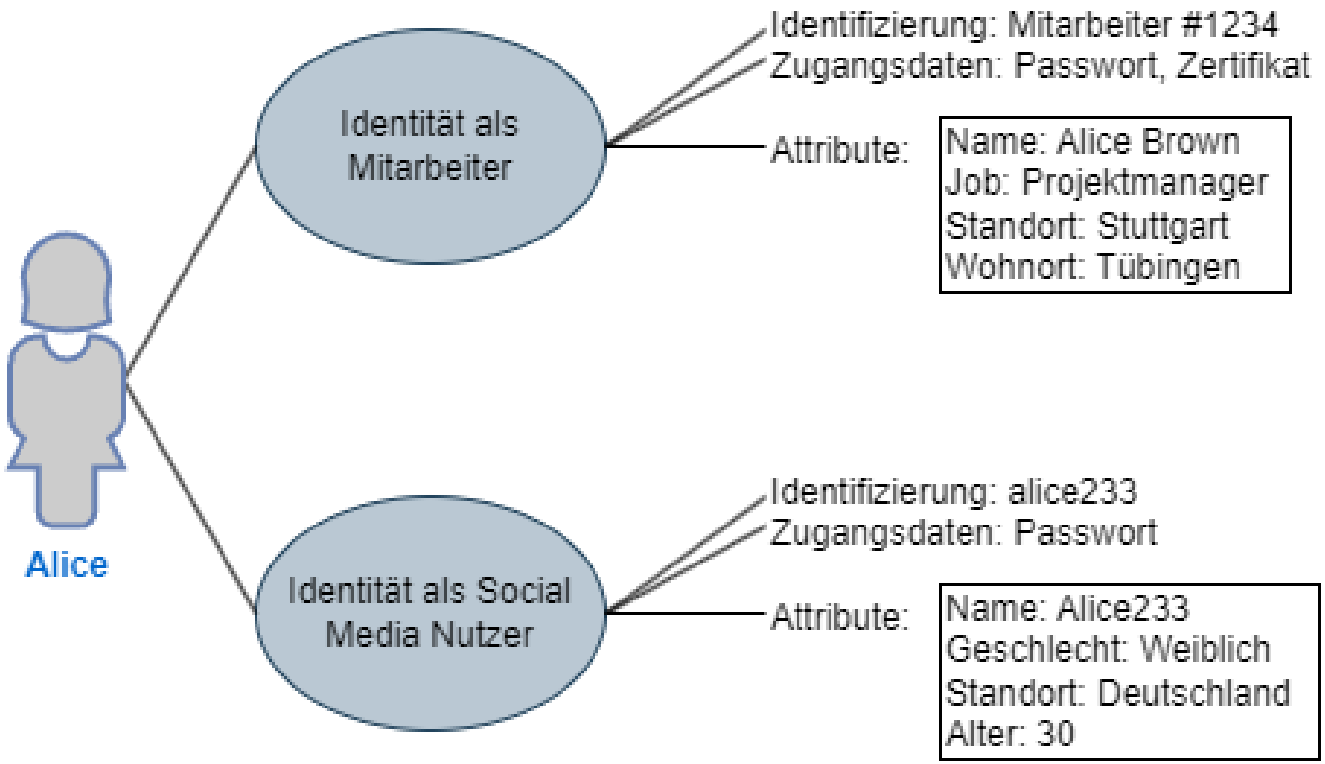

Abbildung: Digitale Identität - Basierend auf Grafik 2.1 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

Identitätsmanagement

- Management von digitalen Identitäten

Identitätsmanagement

- Management von digitalen Identitäten
- Gründe:

Identitätsmanagement

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

Identitätsmanagement

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

Identitätsmanagement

- Management von digitalen Identitäten
- Gründe:
  - Speicherung, Nutzung und Weitergabe von Identitätsinformationen
  - Berechtigungsmanagement
  - Zuordnung von Zutritt und Zugriff zu Entitäten

Identitätsmanagement

- Management von digitalen Identitäten
- Gründe:
  - Speicherung, Nutzung und Weitergabe von Identitätsinformationen
  - Berechtigungsmanagement
  - Zuordnung von Zutritt und Zugriff zu Entitäten
- Aufgabenbereiche:

Identitätsmanagement

- Management von digitalen Identitäten
- Gründe:
  - Speicherung, Nutzung und Weitergabe von Identitätsinformationen
  - Berechtigungsmanagement
  - Zuordnung von Zutritt und Zugriff zu Entitäten
- Aufgabenbereiche:
  - Prozesse (Identitätslebenszyklus)

Identitätsmanagement

- Management von digitalen Identitäten
- Gründe:
  - Speicherung, Nutzung und Weitergabe von Identitätsinformationen
  - Berechtigungsmanagement
  - Zuordnung von Zutritt und Zugriff zu Entitäten
- Aufgabenbereiche:
  - Prozesse (Identitätslebenszyklus)
  - Technik für Authentifizierung

Identitätsmanagement

- Management von digitalen Identitäten
- Gründe:
  - Speicherung, Nutzung und Weitergabe von Identitätsinformationen
  - Berechtigungsmanagement
  - Zuordnung von Zutritt und Zugriff zu Entitäten
- Aufgabenbereiche:
  - Prozesse (Identitätslebenszyklus)
  - Technik für Authentifizierung
  - Compliance mit Gesetzen und Standards

Identitätsmanagement

- Management von digitalen Identitäten
- Gründe:
  - Speicherung, Nutzung und Weitergabe von Identitätsinformationen
  - Berechtigungsmanagement
  - Zuordnung von Zutritt und Zugriff zu Entitäten
- Aufgabenbereiche:
  - Prozesse (Identitätslebenszyklus)
  - Technik für Authentifizierung
  - Compliance mit Gesetzen und Standards
  - Auditierung von Ist vs. Soll

Identitätslebenszyklus

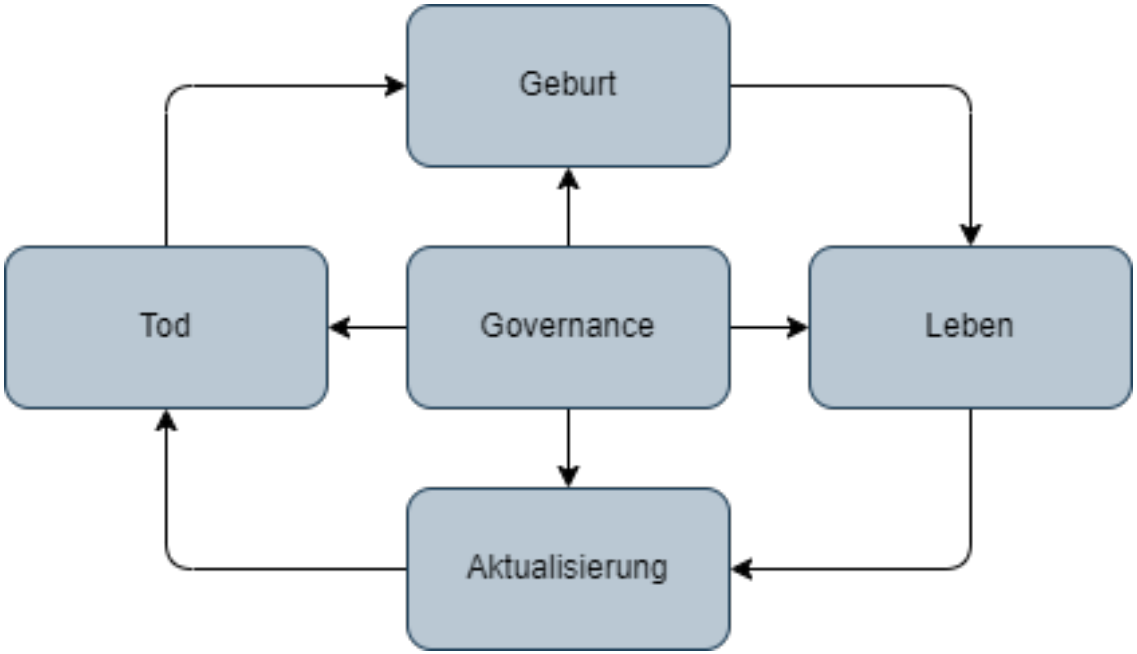

Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

Identitätslebenszyklus

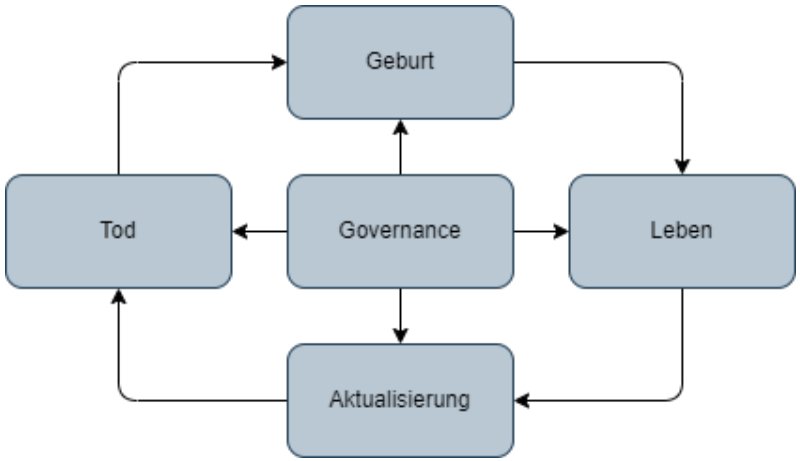

Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

- Geburt: Datensammlung und Validierung, Zugangsdaten

Identitätslebenszyklus

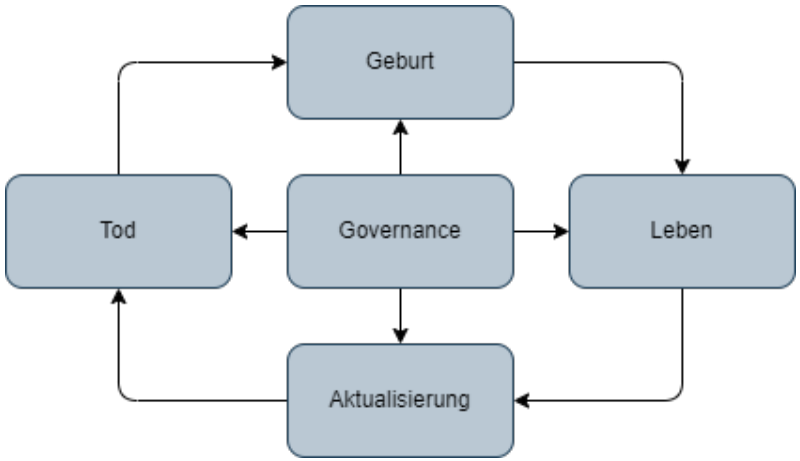

Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

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

Identitätslebenszyklus

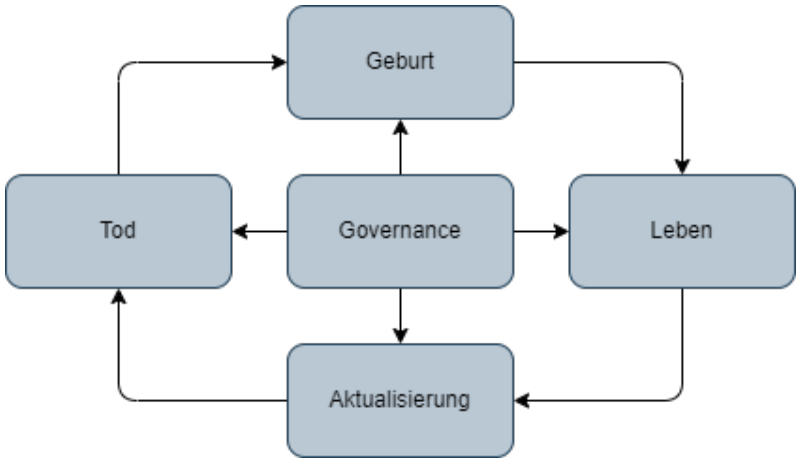

Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

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

Identitätslebenszyklus

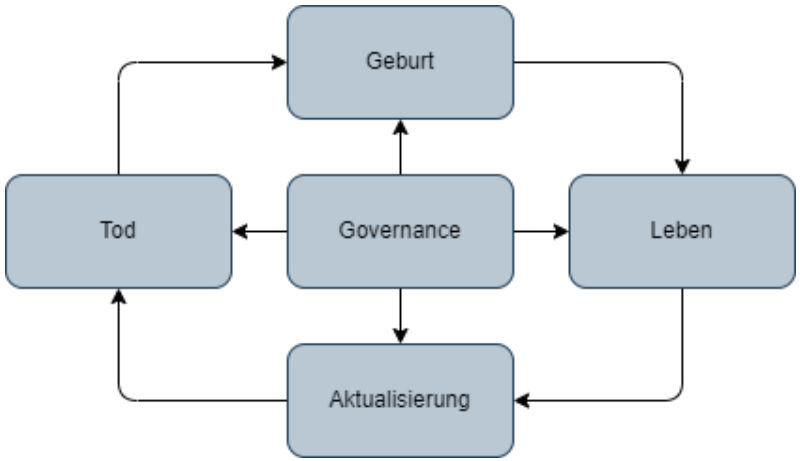

Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

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

Identitätslebenszyklus

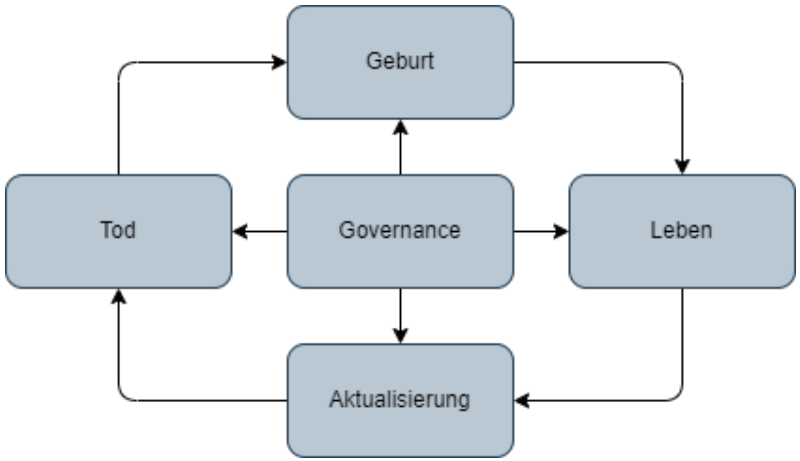

Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

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

Table of Contents

Berechtigung

- Kombination aus Ressource und Operation[2]

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

Berechtigung

- Kombination aus Ressource und Operation[2]
- Beispiele:

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

Berechtigung

- Kombination aus Ressource und Operation[2]
- Beispiele:
  - Wer darf Inhalte des \\ad.hochschule.de Verzeichnisses ändern?

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

Berechtigung

- Kombination aus Ressource und Operation[2]
- Beispiele:
  - Wer darf Inhalte des \\ad.hochschule.de Verzeichnisses ändern?
  - Wer darf in Azure DevOps Repositories löschen?

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

Berechtigung

- Kombination aus Ressource und Operation[2]
- Beispiele:
  - Wer darf Inhalte des \\ad.hochschule.de Verzeichnisses ändern?
  - Wer darf in Azure DevOps Repositories löschen?
  - Wer darf in AWS Zertifikate erstellen?

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

Berechtigung

- Kombination aus Ressource und Operation[2]
- 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?

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

Berechtigungsmanagement

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

Berechtigungsmanagement

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

Berechtigungsmanagement

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

Berechtigungsmanagement

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

Berechtigungsmanagement

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

Berechtigungsmanagement

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

Berechtigungsmanagement

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

Berechtigungsmanagement

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

Berechtigungsmanagement

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe:
  - PoLP/Principle of Least Privilege
  - SoD/Funktionstrennung
- Aufgaben:
  - Berechtigungskonzept auf Unternehmen anpassen - RBAC, ABAC, Kombination ...
  - Technische Umsetzung (Authorisierung)
  - Umsetzung von Complianceanforderungen, methodische Standards
  - Auditierung Ist vs. Soll

Berechtigungsmanagement

- Management von Berechtigungen: Welche Nutzer oder IT-Systeme (digitale Identitäten) dürfen auf welche Ressourcen zugreifen?
- Gründe:
  - PoLP/Principle of Least Privilege
  - SoD/Funktionstrennung
- Aufgaben:
  - Berechtigungskonzept auf Unternehmen anpassen - RBAC, ABAC, Kombination ...
  - Technische Umsetzung (Authorisierung)
  - Umsetzung von Complianceanforderungen, methodische Standards
  - Auditierung Ist vs. Soll
  - Gewährleistung der Rückverfolgbarkeit

Table of Contents

IAM vs CIAM

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

IAM vs CIAM

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

Identitäts- und Berechtigungsmanagement-Systeme

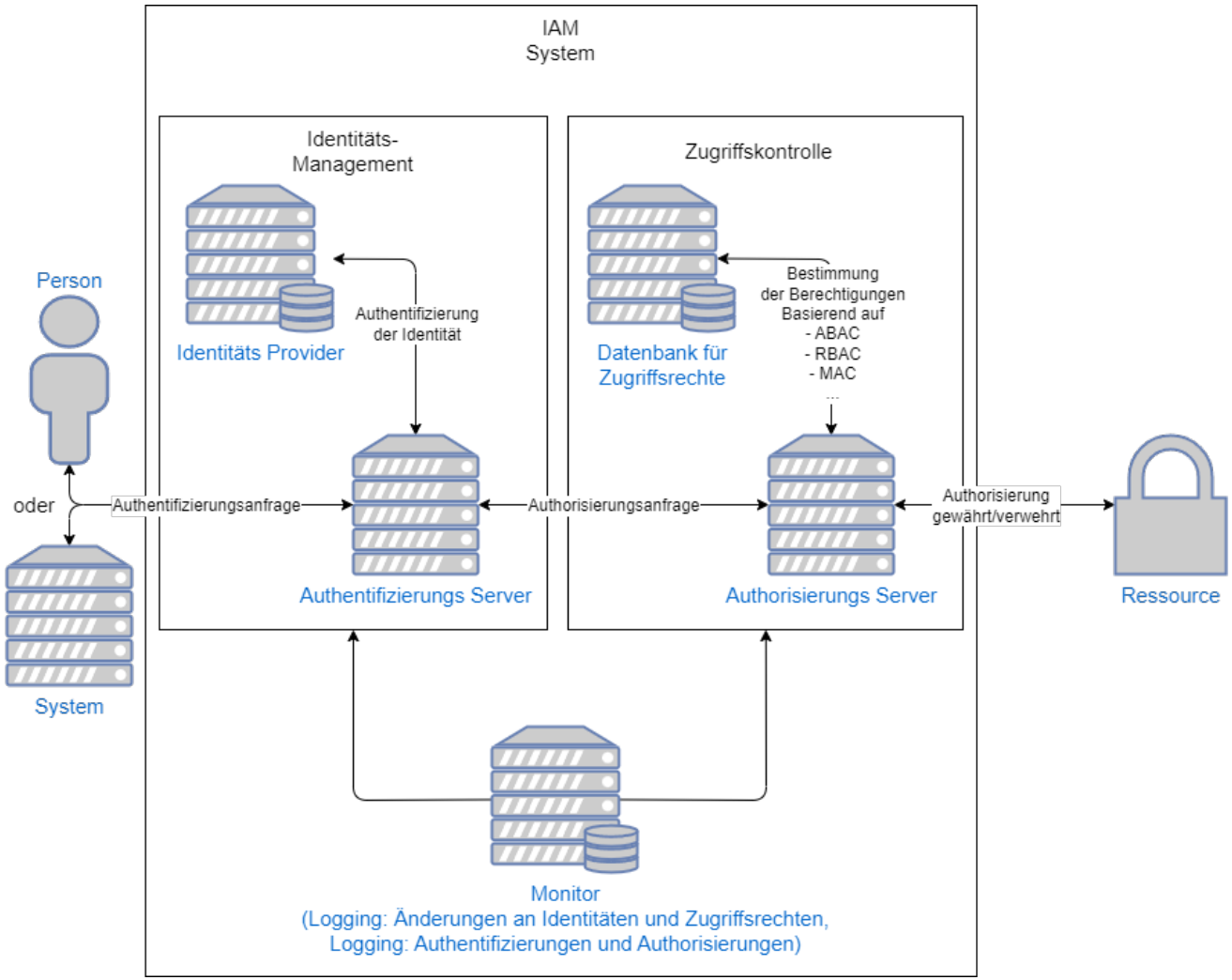

Abbildung: IAM System - Basierend auf Grafik 1 aus „Identity and access management using distributed ledger technology: A survey“ von Fariba Ghaffari, Komal Gilani, Emmanuel Bertin und Noel Crespi

Table of Contents

Operative Aspekte

- CIO: Verantworlich für Prozesse und Technologien

[3] 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.

[4] 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.

[5] Mikko Ylen u. a. "Centralized password management in a global enterprise". Magisterarb. 2004.

Operative Aspekte

- CIO: Verantworlich für Prozesse und Technologien
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzgesetzen und Sicherheitsstandards, Awareness Trainings, interne Audits...[3]

[3] 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.

[4] 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.

[5] Mikko Ylen u. a. "Centralized password management in a global enterprise". Magisterarb. 2004.

Operative Aspekte

- CIO: Verantworlich für Prozesse und Technologien
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzgesetzen und Sicherheitsstandards, Awareness Trainings, interne Audits...[3]
- IT-Betrieb: Implementierung und Wartung der involvierten Technik

[3] 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.

[4] 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.

[5] Mikko Ylen u. a. "Centralized password management in a global enterprise". Magisterarb. 2004.

Operative Aspekte

- CIO: Verantworlich für Prozesse und Technologien
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzgesetzen und Sicherheitsstandards, Awareness Trainings, interne Audits...[3]
- IT-Betrieb: Implementierung und Wartung der involvierten Technik
- Personalabteilung: Identity-Lifecycle Management[4]

[3] 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.

[4] 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.

[5] Mikko Ylen u. a. "Centralized password management in a global enterprise". Magisterarb. 2004.

Operative Aspekte

- CIO: Verantworlich für Prozesse und Technologien
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzgesetzen und Sicherheitsstandards, Awareness Trainings, interne Audits...[3]
- IT-Betrieb: Implementierung und Wartung der involvierten Technik
- Personalabteilung: Identity-Lifecycle Management[4]
- Helpdesk: Hilfe bei Authentifizierung und Authorisierung[5]

[3] 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.

[4] 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.

[5] Mikko Ylen u. a. "Centralized password management in a global enterprise". Magisterarb. 2004.

Table of Contents

Technische Aspekte

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

[6] 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.

[7] IBM. *IBM Security Verify Access Management*. 2024. (Besucht am 28. 05. 2024).

[8] Okta. *Okta Integration Network — Okta*. 2024. (Besucht am 17. 06. 2024).

Technische Aspekte

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta . . .
  - Neue Entwicklung: Cloud (IDaaS - Identity as a Service) im Gegensatz zu traditionellen On-Premise Lösungen[6]

[6] 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.

[7] IBM. *IBM Security Verify Access Management*. 2024. (Besucht am 28. 05. 2024).

[8] Okta. *Okta Integration Network — Okta*. 2024. (Besucht am 17. 06. 2024).

Technische Aspekte

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
  - Neue Entwicklung: Cloud (IDaaS - Identity as a Service) im Gegensatz zu traditionellen On-Premise Lösungen[6]
  - Implementieren Technologien für optimale Umsetzung: Multi Faktor Authentifizierung (OTP, Biometrie), Single Sign On, SAML, OIDC ...

[6] 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.

[7] IBM. *IBM Security Verify Access Management*. 2024. (Besucht am 28. 05. 2024).

[8] Okta. *Okta Integration Network — Okta*. 2024. (Besucht am 17. 06. 2024).

Technische Aspekte

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
  - Neue Entwicklung: Cloud (IDaaS - Identity as a Service) im Gegensatz zu traditionellen On-Premise Lösungen[6]
  - Implementieren Technologien für optimale Umsetzung: Multi Faktor Authentifizierung (OTP, Biometrie), Single Sign On, SAML, OIDC ...
  - Unterstützen Prozesse: Automatisiertes Lifecycle Management, Risikoanalyse, Audit-Management[7]

[6] 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.

[7] IBM. *IBM Security Verify Access Management*. 2024. (Besucht am 28. 05. 2024).

[8] Okta. *Okta Integration Network — Okta*. 2024. (Besucht am 17. 06. 2024).

Technische Aspekte

- Produkte von Konzernen wie Microsoft, SAP, IBM, Okta ...
  - Neue Entwicklung: Cloud (IDaaS - Identity as a Service) im Gegensatz zu traditionellen On-Premise Lösungen[6]
  - Implementieren Technologien für optimale Umsetzung: Multi Faktor Authentifizierung (OTP, Biometrie), Single Sign On, SAML, OIDC ...
  - Unterstützen Prozesse: Automatisiertes Lifecycle Management, Risikoanalyse, Audit-Management[7]
  - Integration von Service Providern: Active Directory, Microsoft Office, AWS, HR Anwendungen[8]

[6] 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.

[7] IBM. *IBM Security Verify Access Management*. 2024. (Besucht am 28. 05. 2024).

[8] Okta. *Okta Integration Network — Okta*. 2024. (Besucht am 17. 06. 2024).

Technische Aspekte

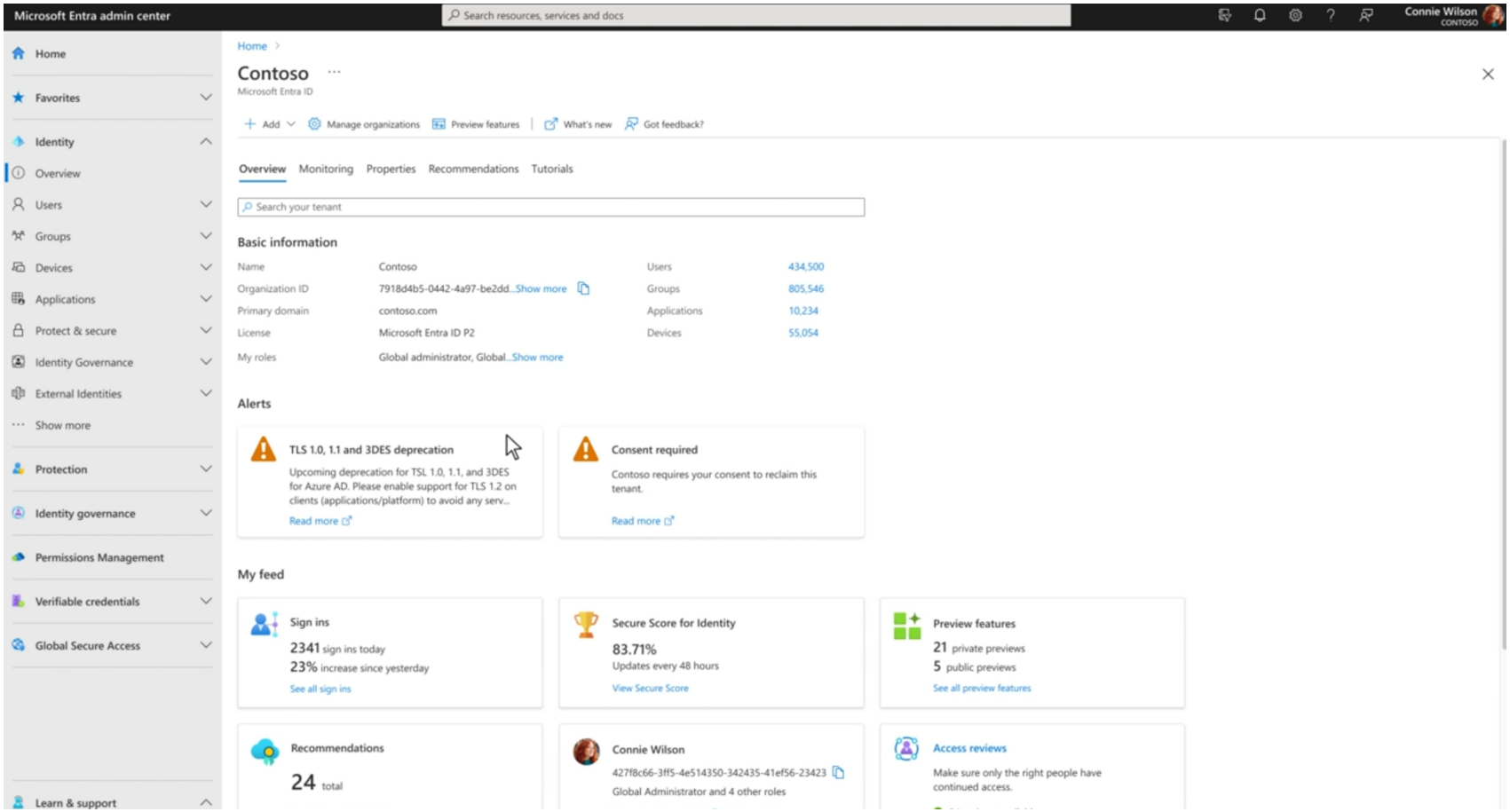

Abbildung: Microsoft Entra ID - von
https://www.microsoft.com/de-de/security/business/microsoft-entra

Technische Aspekte

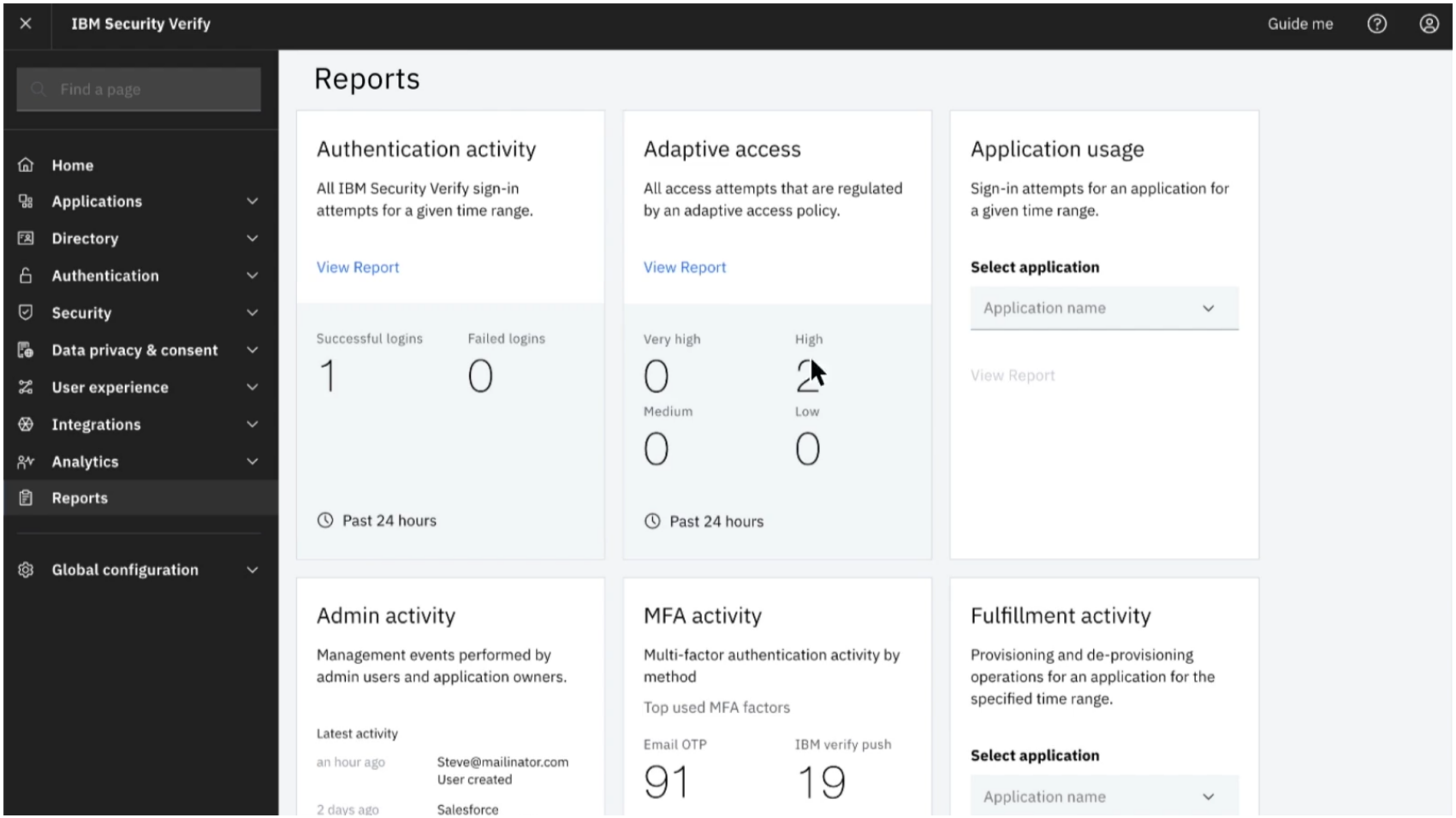

Abbildung: IBM Security Verify - von `https://www.ibm.com/de-de/products/verify-saas`

Technische Aspekte

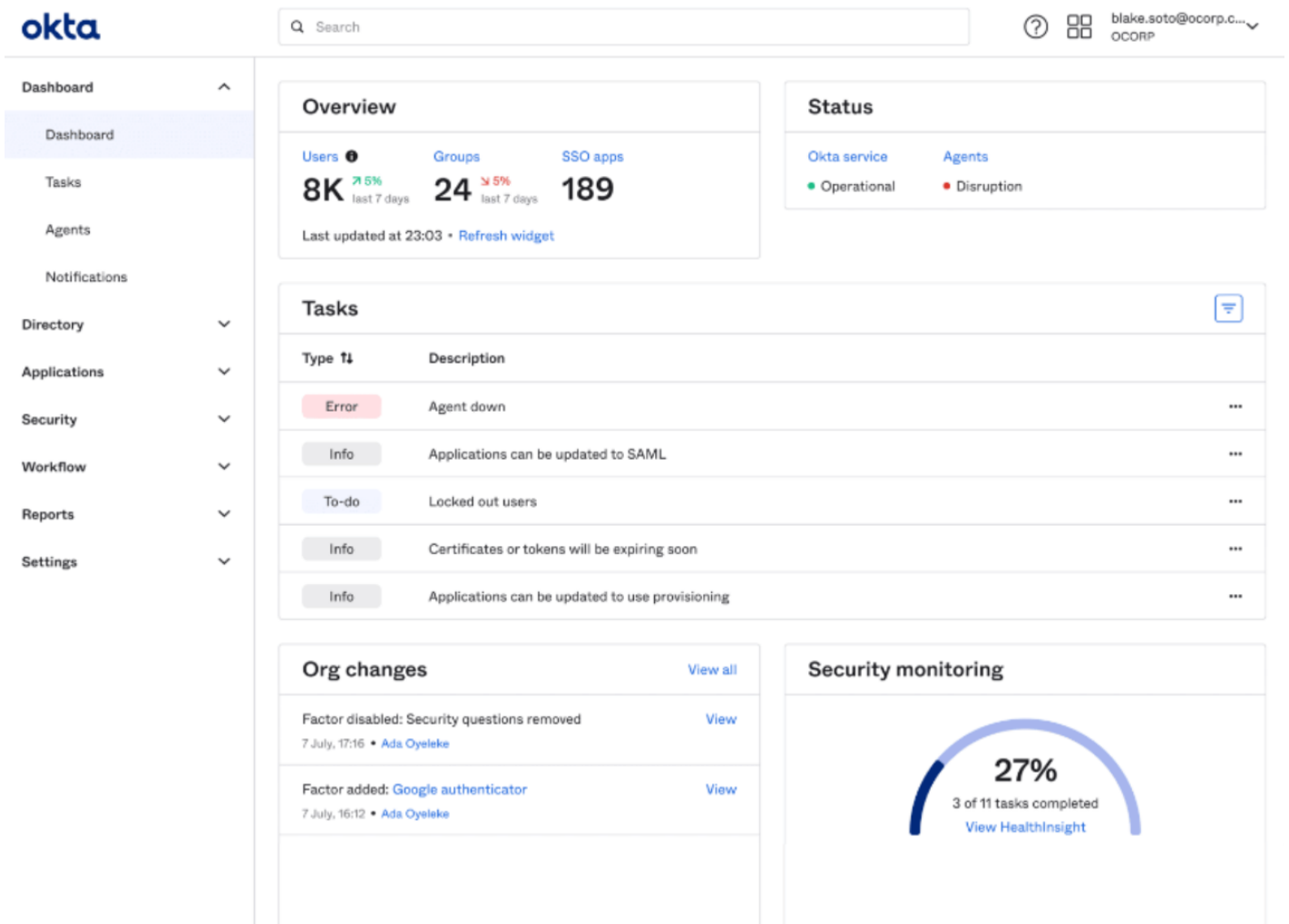

Abbildung: Okta Workforce Identity Cloud - von `https://thectoclub.com/tools/best-identity-and-access-management-solutions/`

Table of Contents

Standards

- ISO/IEC 24760: Identitätsmanagement (Konzepte und operative Strukturen)[9]

[9] ISO. *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).

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

[11] BSI. *BSI - BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)*. Nov. 2017. (Besucht am 28. 05. 2024).

[12] BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. (Besucht am 28. 05. 2024).

[13] NIST. *SP 800-53A Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations*. Jan. 2022. (Besucht am 28. 05. 2024).

Standards

- ISO/IEC 24760: Identitätsmanagement (Konzepte und operative Strukturen)[9]
- ISO 27001: Annex A.9 definiert Zugangssteuerung[10]

[9] ISO. *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).

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

[11] BSI. *BSI - BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)*. Nov. 2017. (Besucht am 28. 05. 2024).

[12] BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. (Besucht am 28. 05. 2024).

[13] NIST. *SP 800-53A Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations*. Jan. 2022. (Besucht am 28. 05. 2024).

Standards

- ISO/IEC 24760: Identitätsmanagement (Konzepte und operative Strukturen)[9]
- ISO 27001: Annex A.9 definiert Zugangssteuerung[10]
- IT-Grundschutz: BSI-Standard 200-1, ORP.4[11][12]

[9] ISO. *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).

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

[11] BSI. *BSI - BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)*. Nov. 2017. (Besucht am 28. 05. 2024).

[12] BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. (Besucht am 28. 05. 2024).

[13] NIST. *SP 800-53A Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations*. Jan. 2022. (Besucht am 28. 05. 2024).

Standards

- ISO/IEC 24760: Identitätsmanagement (Konzepte und operative Strukturen)[9]
- ISO 27001: Annex A.9 definiert Zugangssteuerung[10]
- IT-Grundschutz: BSI-Standard 200-1, ORP.4[11][12]
- NIST 800-53A: Kapitel Access Control Family (AC) und Identification and Authentication Family (IA)[13]

[9] ISO. *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).

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

[11] BSI. *BSI - BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)*. Nov. 2017. (Besucht am 28. 05. 2024).

[12] BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. (Besucht am 28. 05. 2024).

[13] NIST. *SP 800-53A Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations*. Jan. 2022. (Besucht am 28. 05. 2024).

Standards

- ISO/IEC 24760: Identitätsmanagement (Konzepte und operative Strukturen)[9]
- ISO 27001: Annex A.9 definiert Zugangssteuerung[10]
- IT-Grundschutz: BSI-Standard 200-1, ORP.4[11][12]
- NIST 800-53A: Kapitel Access Control Family (AC) und Identification and Authentication Family (IA)[13]
- ...

[9] ISO. *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).

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

[11] BSI. *BSI - BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)*. Nov. 2017. (Besucht am 28. 05. 2024).

[12] BSI. *ORP.4: Identitäts- und Berechtigungsmanagement*. 2021. (Besucht am 28. 05. 2024).

[13] NIST. *SP 800-53A Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations*. Jan. 2022. (Besucht am 28. 05. 2024).

Rechtlich

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

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

[15] EU. *VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES*. Mai 2016. (Besucht am 28. 05. 2024).

Rechtlich

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

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

[15] EU. *VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES*. Mai 2016. (Besucht am 28. 05. 2024).

Rechtlich

- 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

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

[15] EU. *VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES*. Mai 2016. (Besucht am 28. 05. 2024).

Rechtlich

- 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 Daten[14][15]

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

[15] EU. *VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES*. Mai 2016. (Besucht am 28. 05. 2024).

Rechtlich

- 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 Daten[14][15]
- ...

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

[15] EU. *VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES*. Mai 2016. (Besucht am 28. 05. 2024).

Fragen

- Vielen Dank für eure Aufmerksamkeit!

Fragen

- Vielen Dank für eure Aufmerksamkeit!
- Fragen?

Literaturverzeichnis I

[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/Kompendium_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).

Literaturverzeichnis II

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

[5] 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).

[6] IBM. *IBM Security Verify Access Management*. 2024. URL: https://www.ibm.com/products/verify-saas (besucht am 28. 05. 2024).

Literaturverzeichnis III

[7] 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).

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

[9] 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.

[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.

Literaturverzeichnis IV

[11] 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.

[12] NIST. *SP 800-53A Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations*. Jan. 2022. URL: https://csrc.nist.gov/pubs/sp/800/53/a/r5/final (besucht am 28. 05. 2024).

[13] Okta. *Okta Integration Network — Okta*. 2024. URL: https://www.okta.com/de/integrations/ (besucht am 17. 06. 2024).

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

Literaturverzeichnis V

[15] Mikko Ylen u. a. “Centralized password management in a global enterprise”. Magisterarb. 2004.