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

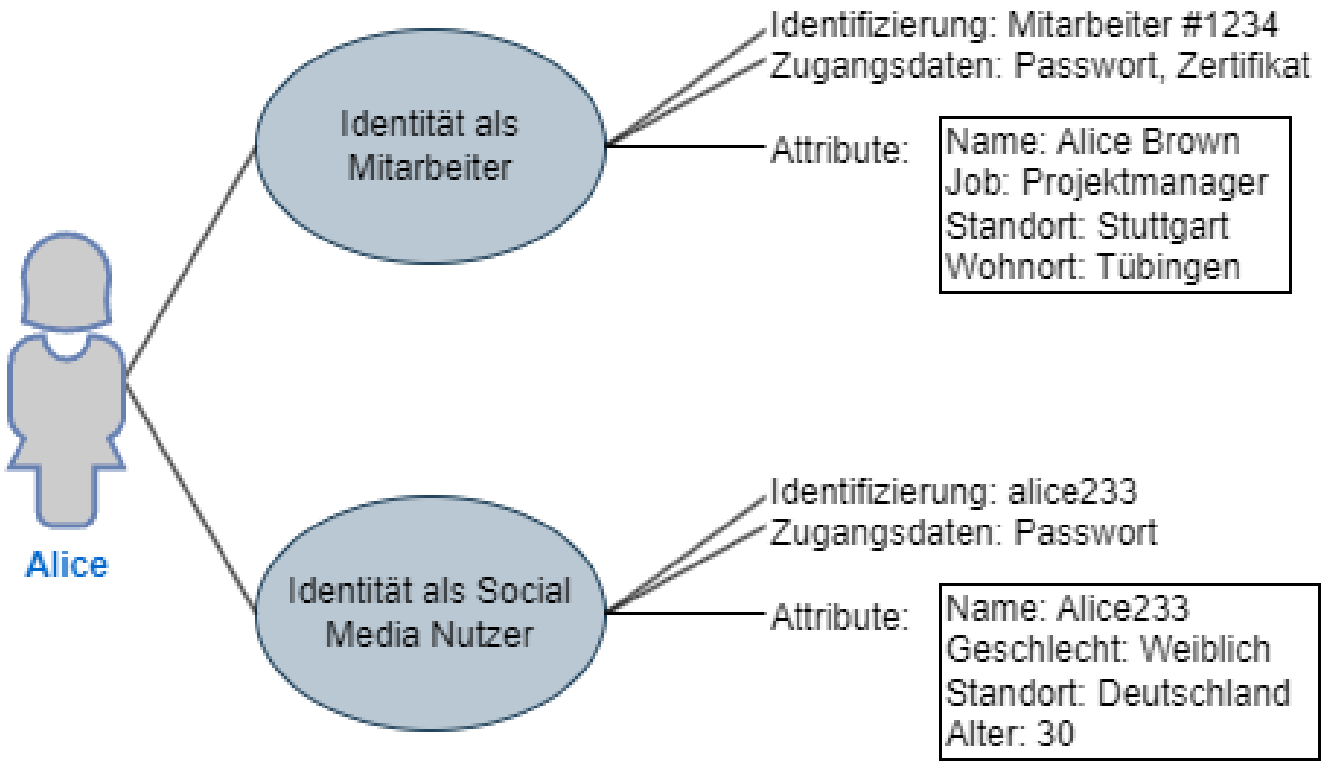

Abbildung: Digitale Identität - Basierend auf Grafik 2.1 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

Identitätsmanagement

- Management von digitalen Identitäten

Identitätsmanagement

- Management von digitalen Identitäten
- Aufgabenbereiche: Umfangreich

Identitätsmanagement

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

Identitätslebenszyklus

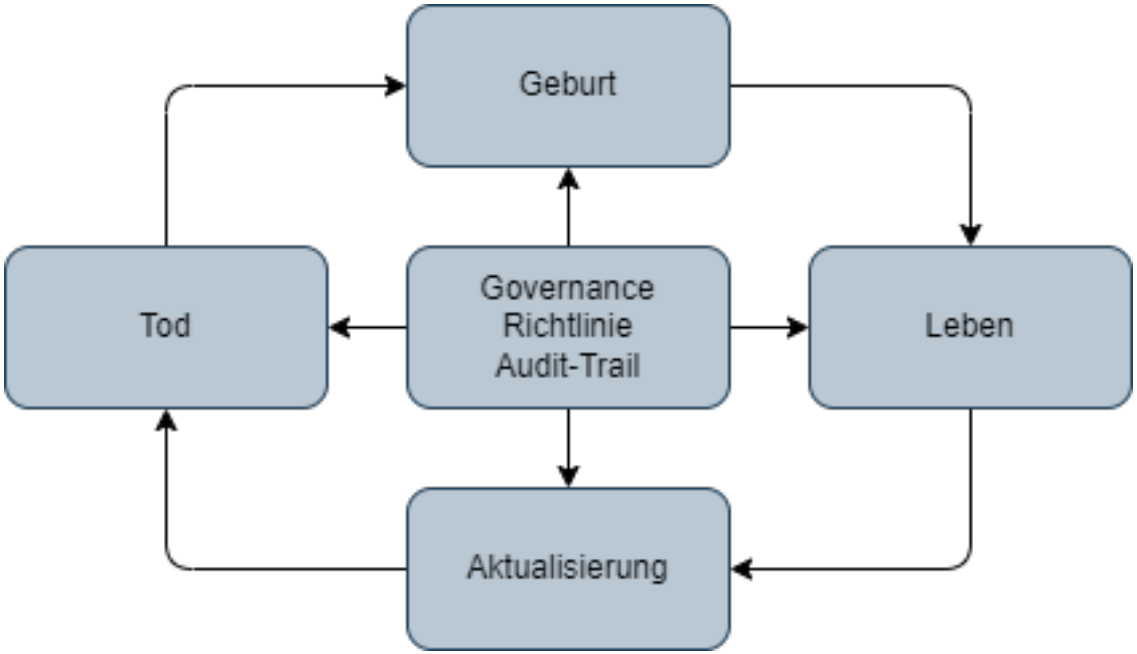

Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

Identitätslebenszyklus

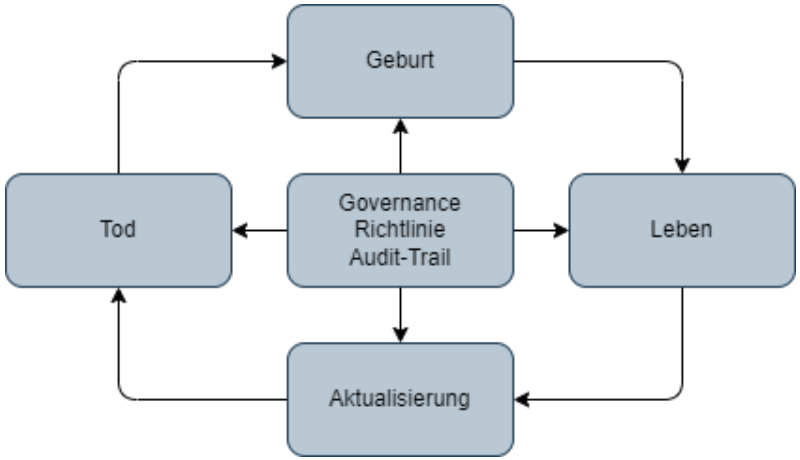

Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

- Geburt: Datensammlung und Validierung, Zugangsdaten

Identitätslebenszyklus

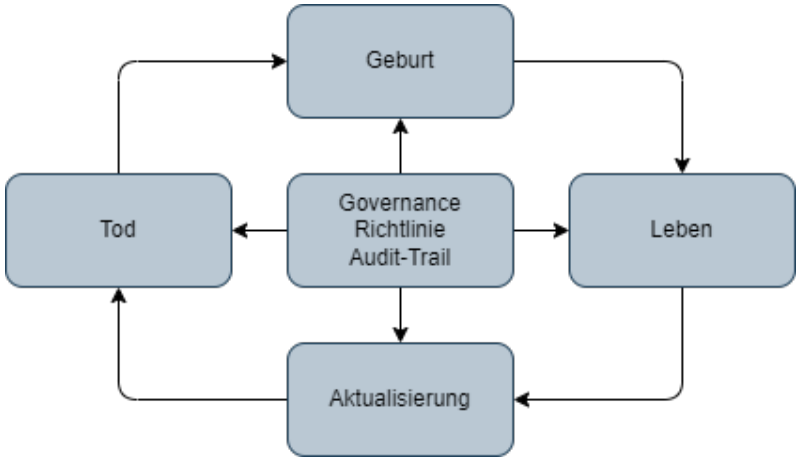

Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

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

Identitätslebenszyklus

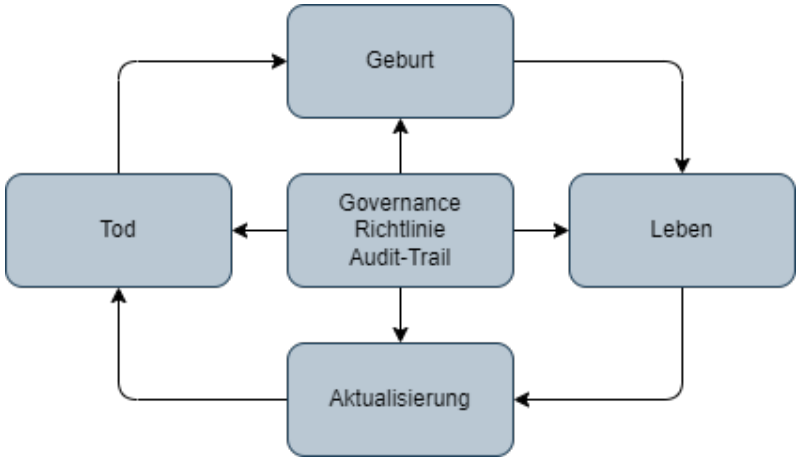

Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

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

Identitätslebenszyklus

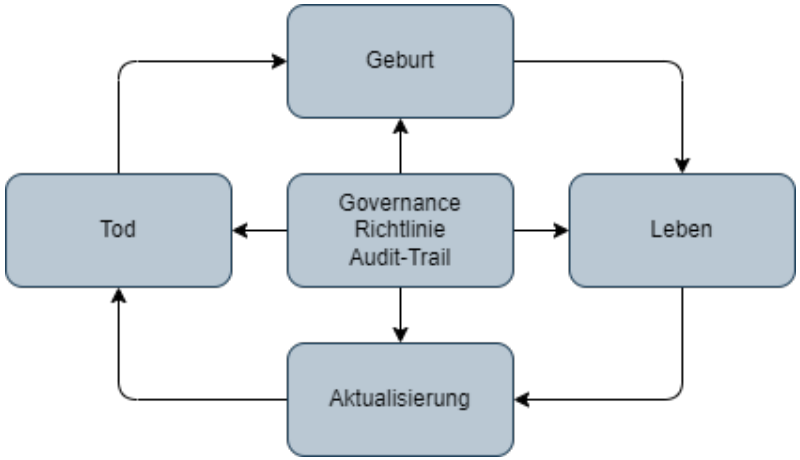

Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

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

Identitätslebenszyklus

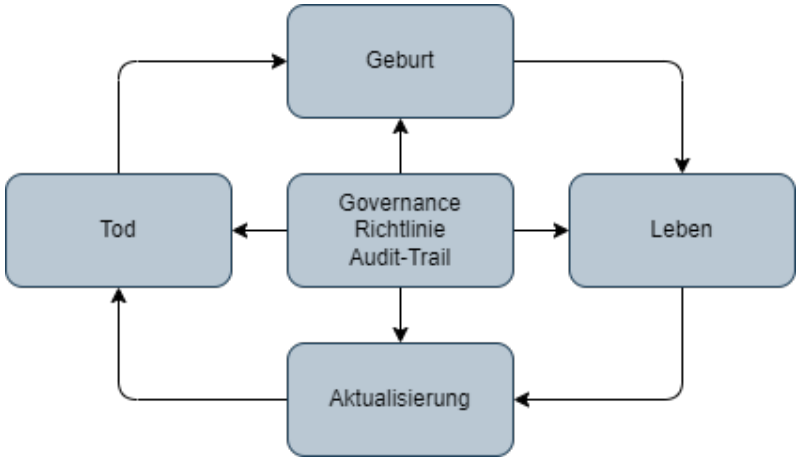

Abbildung: Identitätslebenszyklus - Basierend auf Grafik 2.3 aus „Identity Management Concepts, Technologies, and Systems“ von Elisa Bertino und Kenji Takahashi

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

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. ISBN: 978-3-658-17987-8.

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. ISBN: 978-3-658-17987-8.

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. ISBN: 978-3-658-17987-8.

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. ISBN: 978-3-658-17987-8.

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. ISBN: 978-3-658-17987-8.

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. ISBN: 978-3-658-17987-8.

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?
- Aufgaben:

Berechtigungsmanagement

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

Berechtigungsmanagement

- 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?

Berechtigungsmanagement

- 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)

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

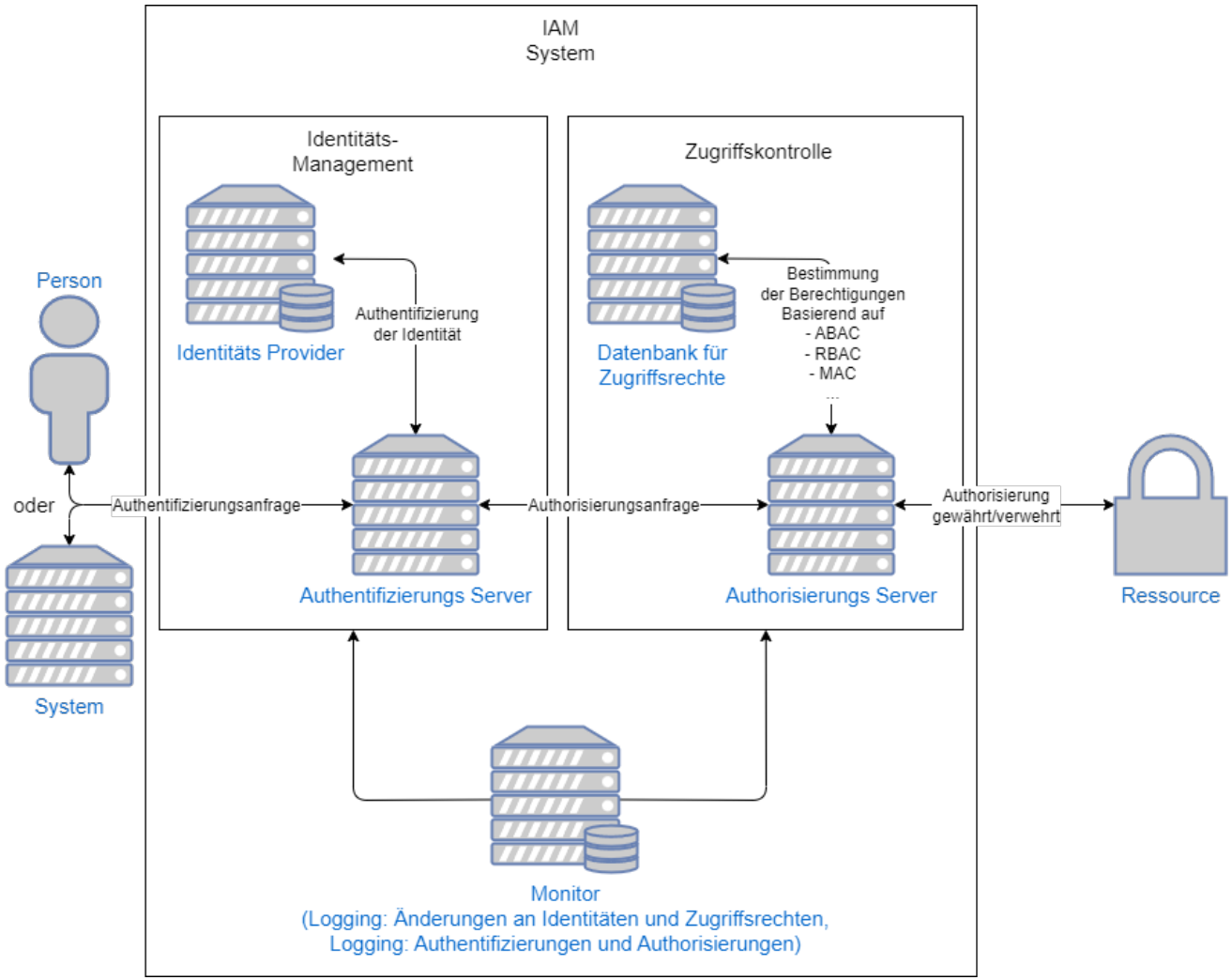

Abbildung: IAM System - Basierend auf Grafik 1 aus „Identity and access management using distributed ledger technology: A survey“ von Fariba Ghaffari, Komal Gilani, Emmanuel Bertin und Noel Crespi

Table of Contents

Operative Aspekte

- CIO: Verantworlich für Prozesse und Technologien

Operative Aspekte

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

Operative Aspekte

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

Operative Aspekte

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

Operative Aspekte

- CIO: Verantworlich für Prozesse und Technologien
- CISO: Bewertung der Prozesse, Überwachung der Compliance mit Datenschutzgesetzen 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

Technische Aspekte

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

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

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
  - Implementieren Technologien für optimale Umsetzung: Multi Faktor Authentifizierung (OTP, Biometrie), Single Sign On

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
  - Implementieren Technologien für optimale Umsetzung: Multi Faktor Authentifizierung (OTP, Biometrie), Single Sign On
  - Unterstützen Prozesse: Automatisiertes Lifecycle Management, Risikoanalyse, Audit-Management

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
  - Implementieren Technologien für optimale Umsetzung: Multi Faktor Authentifizierung (OTP, Biometrie), Single Sign On
  - Unterstützen Prozesse: Automatisiertes Lifecycle Management, Risikoanalyse, Audit-Management
  - Integration von Service Providern: Active Directory, Microsoft Office, AWS, HR Anwendungen

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
  - Implementieren Technologien für optimale Umsetzung: Multi Faktor Authentifizierung (OTP, Biometrie), Single Sign On
  - Unterstützen Prozesse: Automatisiertes Lifecycle Management, Risikoanalyse, Audit-Management
  - Integration von Service Providern: Active Directory, Microsoft Office, AWS, HR Anwendungen
  - ...

Technische Aspekte

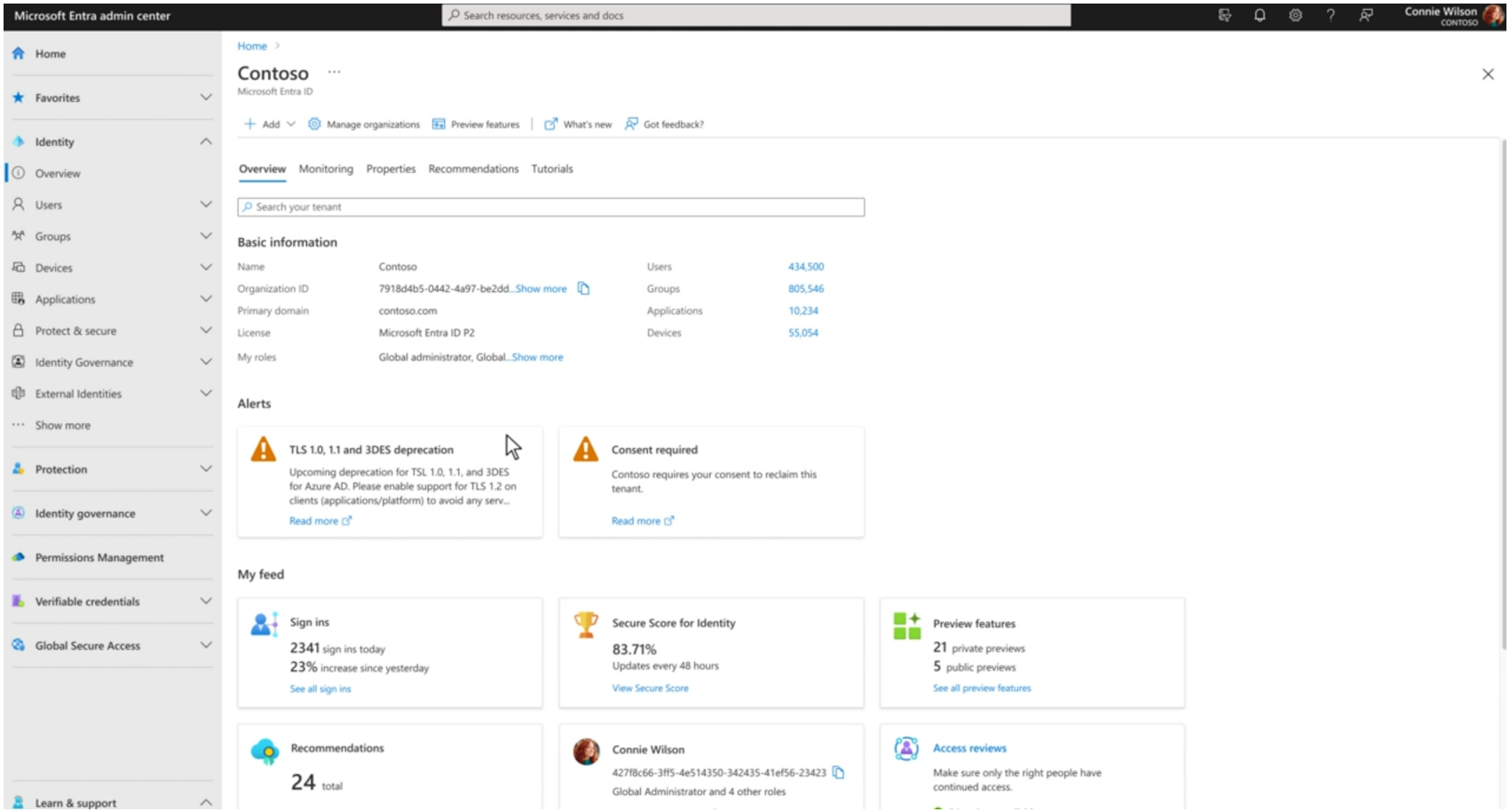

Abbildung: Microsoft Entra ID - von
`https://www.microsoft.com/de-de/security/business/microsoft-entra`

Technische Aspekte

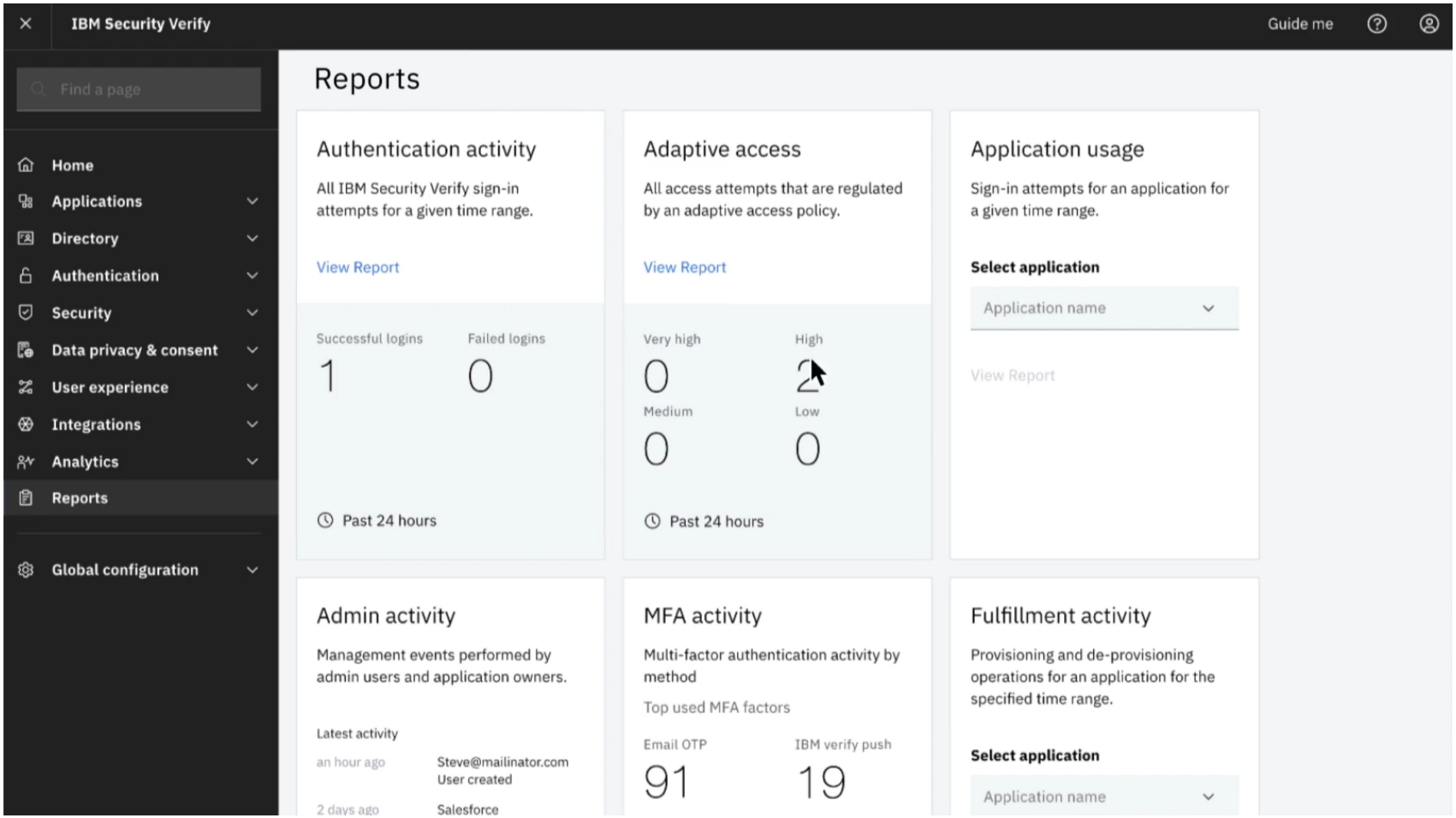

Abbildung: IBM Security Verify - von `https://www.ibm.com/de-de/products/verify-saas`

Technische Aspekte

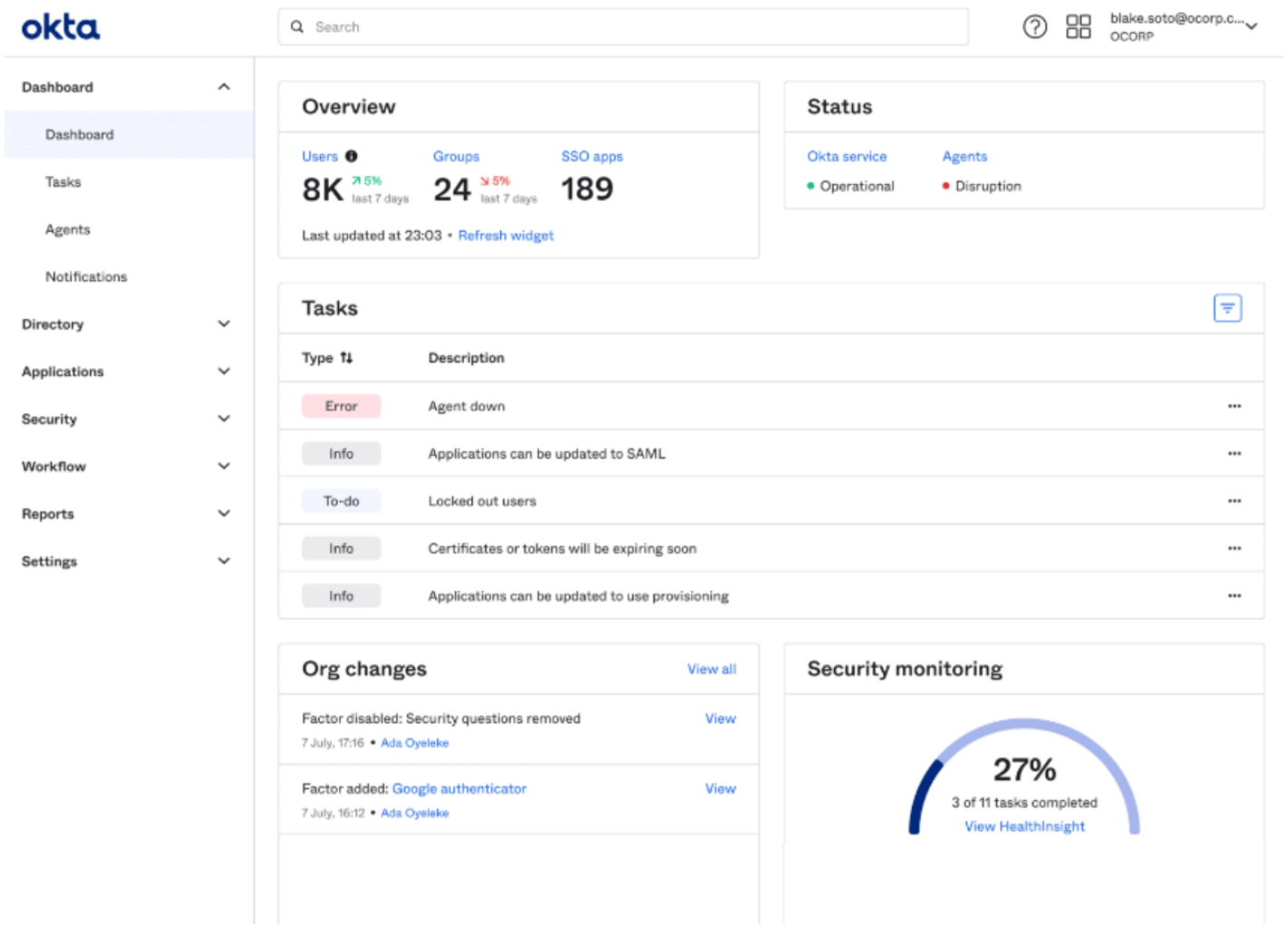

Abbildung: Okta Workforce Identity Cloud - von `https://thectoclub.com/tools/best-identity-and-access-management-solutions/`

Table of Contents

Standards

- ISO 27001: Annex A.9 definiert Zugangssteuerung

Standards

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

Standards

- 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)

Standards

- 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)
- ...

Rechtlich

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

Rechtlich

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

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

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

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
- ...

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] 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.