

Identitäts- und Berechtigungsmanagement

Maximilian Heim

28. Mai 2024

Inhaltsverzeichnis

1	Einleitung	3
1.1	Aufgabenstellung	3
1.2	Forschungsfragen	3
2	Grundlagen	4
2.1	Einordnung	4
2.2	Identität	4
2.3	Identitätsmanagement	6
2.4	Berechtigung	6
2.5	Berechtigungsmanagement	7
2.6	Identitäts- und Berechtigungsmanagement	7
2.7	Erkenntnisse im Kontext von IT-GRC	8
3	Methoden, Technologien und Tools	9
3.1	Betriebliche Motivation	9
3.2	Standards	9
3.3	Methoden und Prozesse	10
3.3.1	Identitäts Lebenszyklus	10
3.4	Technologien und Tools	12
3.4.1	Standardisierte Technologien	12
3.4.2	IAM Lösungen	14
3.5	Erkenntnisse im Kontext von IT-GRC	15
4	Betriebliches Identitäts- und Berechtigungsmanagement	16
4.1	Überblick	16
4.2	Organisatorische Aspekte	16
4.3	Technische Aspekte	17
4.4	Wirtschaftliche Aspekte	17
4.5	Erkenntnisse im Kontext von IT-GRC	20
5	Fazit	20
5.1	Zusammenfassung	20
5.2	Beantwortung der Forschungsfragen	20
6	Eidesstattliche Versicherung	23

1 Einleitung

1.1 Aufgabenstellung

Diese Seminararbeit wurde im Rahmen der Vorlesung IT-GRC angefertigt. Ziel der Arbeit ist es die in Kapitel 1.2 definierten Forschungsfragen zu beantworten. Die Forschungsfragen zielen darauf ab wichtige Aspekte des betrieblichen Identitäts- und Berechtigungsmanagements im Kontext der IT-GRC zu beleuchten.

1.2 Forschungsfragen

Im Rahmen der Seminararbeit wurden 7 Forschungsfragen definiert, diese sind im Folgenden aufgeführt.

- Was versteht man unter den Begriffen „Identität“ sowie „Identitätsmanagement“ und welche Zielstellung wird dabei verfolgt?
- Was versteht man unter den Begriffen „Berechtigung“ sowie „Berechtigungsmanagement“ und welche Zielstellung wird dabei verfolgt?
- Welche Standards, Methoden, Technologien und Tools lassen sich differenzieren?
- Welche Aufgaben und Prozesse sind im Kontext von Identitäts und Berechtigungsmanagement zu bearbeiten?
- Welche betrieblichen Anwendungsfälle zeigen die Bedeutung des Identitäts und Berechtigungsmanagements auf?
- Wie wird das Identitäts und Berechtigungsmanagement im Kontext der Sicherheit in der Informationstechnik eingesetzt?
- Wer hat im Unternehmen typischerweise die Zuständigkeit für Identitäts und Berechtigungsmanagement und wer führt diese Aufgaben operativ durch?

2 Grundlagen

2.1 Einordnung

Das Identitäts- und Berechtigungsmanagement ist eine zentrale Disziplin in der Informationssicherheit. Das Identitäts- und Berechtigungsmanagement besteht aus Richtlinien, Prozessen und Technologien zur Verwaltung von Identitäten und Zugriffssteuerung. Identitätsmanagement und Berechtigungsmanagement sind zwei unterschiedliche Disziplinen, jedoch werden diese meist zusammen angewendet. (vgl. Mohammed 2017 Seite 1) Es wird häufig zwischen Identitäts- und Berechtigungsmanagement (IAM) und Customer Identitäts- und Berechtigungsmanagement (CIAM) unterschieden. Bei IAM geht es um die Authentifikation und Zugriffskontrolle im Unternehmen. Im Kontrast behandelt das CIAM die Authentifikation und Zugriffskontrolle von Nutzern außerhalb vom Unternehmen. (vgl. Liveretos und Draganov 2022 Seite 2)

2.2 Identität

Um den Begriff Identitätsmanagement zu definieren sollte zuerst der Begriff der Identität definiert werden. In der Philosophie wird Identität über die Ununterscheidbarkeit von Dingen definiert. Nach dem Identitätsprinzip sind zwei Dinge genau dann identisch wenn sich zwischen ihnen keine Unterschiede finden lassen, d.h. zwei Personen oder zwei Computersysteme sind nie identisch. Hierbei geht es um die Fragestellung „wer/was bist du?“. Im Kontext des Identitätsmanagements handelt es sich hier um digitale Identitäten, d.h. eine Menge an Attributen und Rollen die einer Person, einem IT-System oder einer Anwendung zugeordnet werden können, inklusive einem Bezeichner und Zugangsdaten die zur Nutzung der Identität notwendig sind. Ein Subjekt (Person, System) kann mehreren digitalen Identitäten zugeordnet sein. (vgl. Bertino und Takahashi 2010 Seite 21-23) Dieser Sachverhalt ist in Abbildung 1 dargestellt.

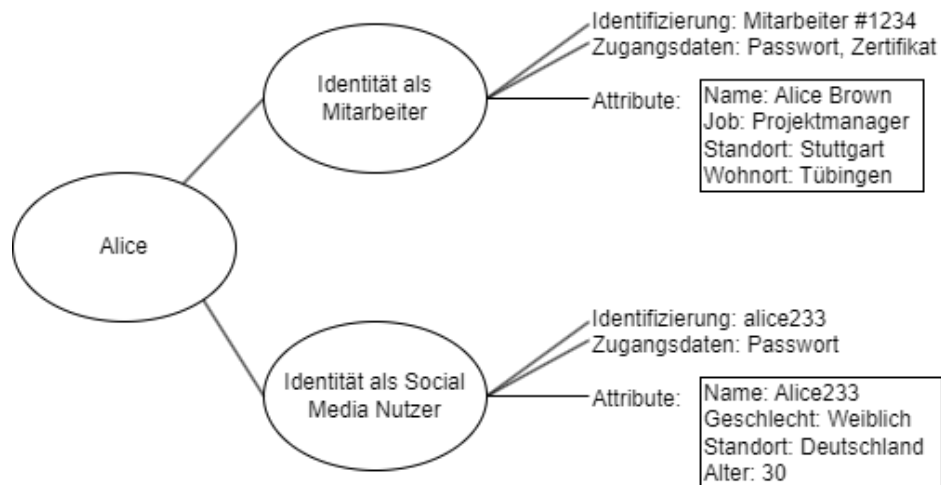


Abbildung 1: Digitale Identität - In Anlehnung an Grafik 2.1 aus Identity Management Concepts, Technologies, and Systems von Elisa Bertino und Kenji Takahashi

In der Informationstechnik wird der Beweis über die eigene Identität, basierend auf Bezeichner und Zugangsdaten als Authentifizierung bezeichnet. Es haben sich verschiedenste Authentifizierungsverfahren durchgesetzt von denen im Folgenden einige vorgestellt werden. (vgl. Tsolkas und Schmidt 2017 Kapitel 7: Zugriffskontrolle über Authentifizierung)

Authentifizierungsverfahren

- Passwörter und Pins sind die wohl bekanntesten Arten der Authentifizierung. Jedoch ist es auch eine der unsichersten Arten da diese gerne mehrfach verwendet werden oder bei unzureichender Länge geknackt werden können
- Tokens sind eine andere Art der Authentifizierung die auf Besitz und Wissen basieren und daher sicherer sind wie rein wissensbasierte Verfahren wie Passwörter. Hierbei wird ein Gerät verwendet welches nach Entsperrung mittels Pin/Passwort ein Einmalpasswort ausgibt oder automatisch die Authentifizierung freigibt
- Eine weiteres Beispiel für Authentifizierung ist die Biometrie. Hierbei

werden z.B. der Fingerabdruck, die Retina oder die Stimme einer Person verwendet um diese zu authentifizieren

2.3 Identitätsmanagement

Identitätsmanagement ist die Verwaltung von digitalen Identitäten im Zuge der Authentifizierung und Weitergabe von Identitätsinformationen. (vgl. Bertino und Takahashi 2010 Seite 23) Die Aufgaben im Bereich des Identitätsmanagements sind vielfältig. Es gibt unterschiedliche Definitionen von den Teilbereichen des Identitätsmanagements. Jedoch lassen sich aus den verschiedenen Quellen grundlegende Aufgaben extrahieren welche im Rahmen des Identitätsmanagements durchgeführt werden müssen. Die Aufgabenbereiche sind im Folgenden aufgelistet.

- Identity Lifecycle Management: Management von Prozessen für die Provisionierung, Änderung und Deprovisionierung von digitalen Identitäten (vgl. Bertino und Takahashi 2010 Seite 29-37)
- Technologie: Planung, Implementierung und Wartung der Infrastruktur zur Speicherung und Authentifizierung von digitalen Identitäten (vgl. Bertino und Takahashi 2010 Seite 45)
- Compliance: Identifikation von Standards und Gesetzen welche eingehalten werden müssen, Definition von Prozessen zur Einhaltung der Compliance Vorgaben (vgl. Bertino und Takahashi 2010 Seite 17)
- Audit: Auditierung der Compliance Vorgaben im Rahmen der Identifikation von Abweichungen zu den Vorgaben und Speicherung von Transaktionen zur Nachverfolgbarkeit (vgl. Bertino und Takahashi 2010 Seite 17)

2.4 Berechtigung

Berechtigungen oder auch Zugriffsberechtigungen beschreiben welche Identitäten auf welche Ressourcen zugreifen dürfen. Eine Berechtigung besteht aus einer zu berechtigenden Ressource und aus einer zu berechtigenden Operation für diese Ressource. Beispiele hierfür sind der Schreibzugriff auf eine Datenbank, der Lesezugriff auf Dokumente oder der Konfiguration von Rechnersystemen. (vgl. Tsolkas und Schmidt 2017 Seite 3-4) Dieser Prozess findet

nach der Authentifizierung statt. Hierbei geht es um die Fragestellung „was ist erlaubt?“. Die Kontrolle der Berechtigungen basierend auf einer Identität wird Zugriffskontrolle oder auch Autorisierung genannt. (vgl. Tsolkas und Schmidt 2017 Seite 161-162)

2.5 Berechtigungsmanagement

Berechtigungsmanagement ist verantwortlich für die Festlegung welche Nutzer/Entitäten auf welche Ressourcen Zugriff haben und die Kontrolle dieser Berechtigungen. (vgl. BSI 2021b Seite 1) Das Ziel hierbei ist das Least-Privilege-Prinzip (PoLP) umzusetzen. (vgl. BSI 2021b Seite 2) Die Definitionen der Aufgabenbereiche im Berechtigungsmanagement divergieren wie auch beim Identitätsmanagement je nach Quelle. Jedoch lassen sich ebenso verschiedene Aufgabenbereiche identifizieren, diese sind im Folgenden vorgestellt.

- **Berechtigungssteuerung:** Management von Prozessen für die Provisierung, Änderung und Deprovisionierung von Berechtigungen (vgl. BSI 2021b Seite 1 und Tsolkas und Schmidt 2017 Seite 176)
- **Technologie:** Planung, Implementierung und Wartung der Infrastruktur zur Berechtigungskontrolle (vgl. Tsolkas und Schmidt 2017 Seite 177)
- **Compliance:** Identifikation von Standards und Gesetzen welche eingehalten werden müssen, Definition von Prozessen zur Einhaltung der Compliance Vorgaben (vgl. Conta 2017 Seite 10-31)
- **Audit:** Auditierung der Compliance Vorgaben im Rahmen der Identifikation von Abweichungen zu den Vorgaben und Speicherung von Transaktionen zur Nachverfolgbarkeit (vgl. Tsolkas und Schmidt 2017 Seite 21)

2.6 Identitäts- und Berechtigungsmanagement

Die systematische Unterteilung von Identitäts- und Berechtigungsmanagement erweist sich als schwierig da es hierbei viele Abhängigkeiten gibt. Ein besseres Gesamtbild ergibt sich durch die Betrachtung der Prozesse im Kontext des kombinierten Identitäts- und Berechtigungsmanagements. In Abbildung 2 ist der Ablauf der Zugriffssteuerung im Rahmen eines IAM Systems illustrativ dargestellt.

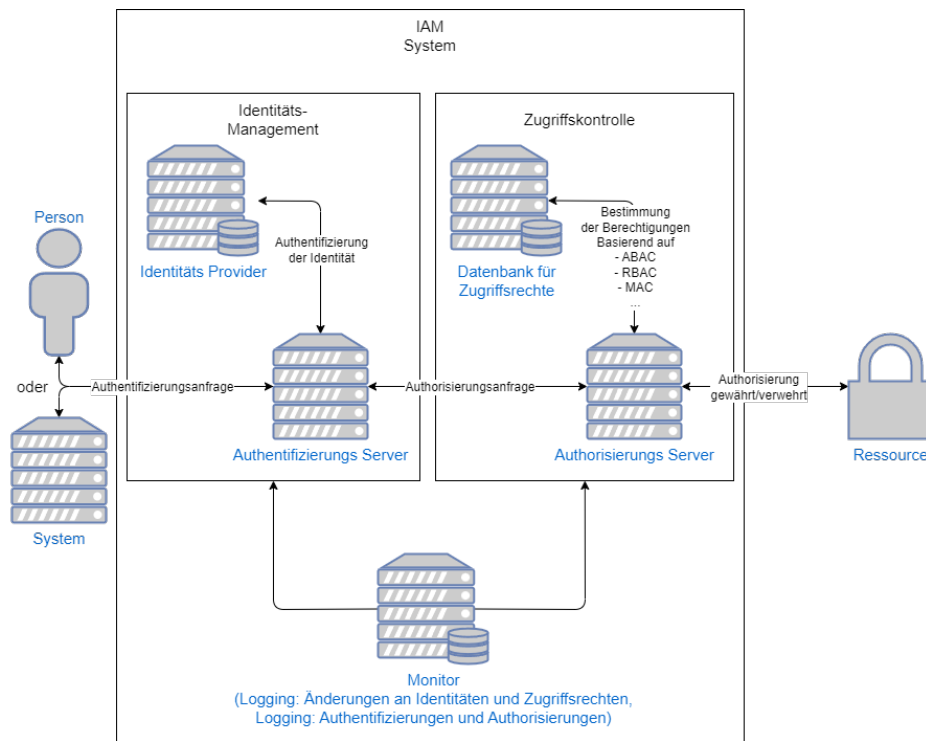


Abbildung 2: Illustration der Zugriffssteuerung im Rahmen eines IAM Systems - In Anlehnung an Ghaffari u. a. 2022 Abbildung 1

2.7 Erkenntnisse im Kontext von IT-GRC

- Die Nutzung von Identitäts- und Berechtigungsmanagement spielt eine zentrale Rolle im unternehmensweiten Risikomanagement. Durch die Steuerung welche logischen Identitäten auf welche Ressourcen zugreifen kann können eine Vielzahl an beabsichtigter und unbeabsichtigter Sicherheitsrisiken minimiert werden.
- Das Identitäts- und Berechtigungsmanagement ist ein tiefgreifendes Thema in der IT-Governance und besteht aus verschiedenen Prozessen, Technologien und Gesetzen welche im Kontext der ganzen Unternehmenstätigkeiten betrachtet werden müssen.

3 Methoden, Technologien und Tools

3.1 Betriebliche Motivation

3.2 Standards

BSI Das Bundesamt für Sicherheit der Informationstechnik (BSI) definiert den IT-Grundschutz. Dieser besteht aus den BSI-Standards und dem IT-Grundschutz-Kompendium. (vgl. BSI 2017a) In BSI-Standard 200-1 werden Sicherheitsmaßnahmen definiert die zur Behandlung der Risiken geeignet sind, in diesen Sicherheitsmaßnahmen wird das Identitäts- und Berechtigungsmanagement als Sicherheitsmaßnahme aufgeführt. (vgl. BSI 2017b Seite 35) In Bezug auf den BSI-Standard definiert das IT-Grundschutz-Kompendium Prozessbausteine zur Umsetzung des ISMS.(vgl. BSI 2023a) Hier wird im Prozessbaustein „ORP.4 Identitäts- und Berechtigungsmanagement“ auf verschiedene Anforderungen für die Umsetzung von Identitäts- und Berechtigungsmanagement eingegangen. Kapitel 3.1 definiert Basis-Anforderungen welche umgesetzt werden müssen. Kapitel 3.2 definiert Standard-Anforderungen welche umgesetzt werden sollten. Kapitel 3.3 definiert Anforderungen welche bei erhöhtem Schutzbedarf umgesetzt werden sollten. (vgl. BSI 2021b) Zusätzlich zu ORP.4 gibt es das Dokument „Umsetzungshinweise zum Baustein: ORP.4. Identitäts- und Berechtigungsmanagement“ welches spezifische Maßnahmen zur Umsetzung von ORP.4 definiert. (vgl. BSI 2022)

ISO 27001 Annex A.9 ISO 27001 definiert mit Anhang A.9 Kontrollen für die Zugangskontrolle. Das Kapitel ist in die Unterkapitel „9.1 Geschäftsanforderungen an die Zugangssteuerung“, „9.2 Benutzerzugangsverwaltung“, „9.3 Benutzerverantwortlichkeiten“ und „9.4 Zugangssteuerung für Systeme und Anwendungen“ unterteilt. (vgl. Kersten u. a. 2020 Seite 121-138) Die Maßnahmen des oben erwähnten IT-Grundschutz-Kompendiums eignen sich zur Umsetzung der ISO 27001 Kontrollen. Somit kann eine ISO 27001 Zertifizierung auf Basis vom IT-Grundschutz umgesetzt werden. (vgl. BSI 2023b) Eine Gegenüberstellung des Anhangs A.9 zu den Prozessbausteinen lässt sich im Dokument „Zuordnungstabelle: Zuordnung ISO/IEC 27001 zum IT-Grundschutz“ finden. (vgl. BSI 2021a)

ISO/IEC 24760 Eine speziell für Identitätsmanagement erstellte Norm ist ISO/IEC 24760. Hierbei werden Konzepte und operative Strukturen zur

korrekten Umsetzung von Identitätsmanagement definiert. ISO 2023

NIST 800-53A Das National Institute of Standards and Technology (NIST) publizierte die „NIST Special Publication 800-53A - Assessing Security and Privacy Controls in Information Systems and Organizations“. Dieses Dokument stellt Prozesse und Methoden für die Bewertung von Sicherheits- und Datenschutzmaßnahmen vor. Im Kapitel „Security and Privacy Assessment Procedures“ wird im Unterkapitel 4.1 „Access Control Family (AC)“ auf Zugangskontrolle und im Unterkapitel 4.7 „Identification and Authentication Family (IA)“ auf Identifizierung und Authentifizierung eingegangen.

3.3 Methoden und Prozesse

3.3.1 Identitäts Lebenszyklus

Ein zentraler Prozess welcher im Rahmen des Identitätsmanagements definiert und umgesetzt werden muss ist der Identitäts Lebenszyklus. Dieser enthält die grundlegenden Elemente Geburt, Leben, Änderung, Tod und Governance. Der Prozess ist in Abbildung 3 dargestellt und wird nachfolgend genauer beschrieben. Bertino und Takahashi 2010

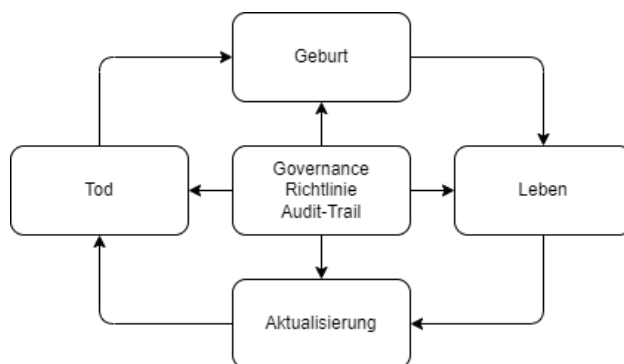


Abbildung 3: Identity Life Cycle - In Anlehnung an Identity Management Concepts, Technologies, and Systems von Elisa Bertino und Kenji Takahashi

Geburt

Festlegung und Überprüfung von Attributen Der erste Schritt in der Geburt einer Identität ist die Sammlung relevanter Attribute wie Na-

me, Geburtsdatum, Wohnsitz, Rolle im Unternehmen etc. und Überprüfung dieser. Bertino und Takahashi 2010

Festlegen von Anmeldeinformationen Um dem Subjekt Zugriff auf die provisionierte Identität zu geben müssen Bezeichner (z.B. E-Mail Adressen oder Nutzernamen) und geeignete Verfahren zur Authentifikation festgelegt werden. So werden in diesem Schritt z.B. Einmalpasswörter für die initiale Anmeldung vergeben oder der Fingerabdruck der zu authentifizierenden Person gespeichert. Bertino und Takahashi 2010

Abschließende Erstellung Nachdem alle relevanten Informationen zur Erstellung der Identität gesammelt wurden kann die Identität erstellt werden. Bertino und Takahashi 2010

Leben

Authentifizierung Die Authentifizierung der eigenen Identität ermöglicht die gesicherte Nutzung von Ressourcen. Bertino und Takahashi 2010

Weitergabe von Informationen Verfahren zur Weitergabe von Informationen sind ein zentraler Aspekt beim Ausleben einer digitalen Identität. Bertino und Takahashi 2010

Aktualisierung

Änderungen Bei Änderung von Attributen wie z.B. Rollen im Unternehmen, Wohnort oder Namensänderung müssen die Attribute schnellstmöglich aktualisiert werden um die Integrität dieser zu gewährleisten. Zugangsdaten wie neu ausgestellte Zertifikate oder geänderte Passwörter müssen ebenso aktualisiert werden um die Authentifizierung zu gewährleisten. Bertino und Takahashi 2010

Tod

Entzug von Zugangsrechten Bei der Kündigung oder Beurlaubung von Mitarbeitern oder bei der Dekommisionierung von Systemen muss der Zugriff auf Ressourcen aufgehoben werden um Sicherheitsrisiken zu verhindern. In diesem Szenario ist es jedoch auch wichtig die Identitätsinformationen weiterhin zu persistieren um für zukünftige Untersuchungen wie z.B. des Audit-Trails eine Zuordnung zu haben. Bertino und Takahashi 2010

Governance

Richtlinien Die Administration, Nutzung und Weitergabe von Identitätsinformationen muss klar durch Richtlinien definiert sein. Bertino und Takahashi 2010

Audit Trail Jegliche Transaktionen bezüglich Zugriff, Änderung oder Weitergabe von Identitätsinformationen sollten aufgezeichnet werden um die Rückverfolgbarkeit zu gewährleisten. Bertino und Takahashi 2010

3.4 Technologien und Tools

IAM Tools ersetzen nicht die Einhaltung von Standards und die sorgfältige Planung von IAM Prozessen. Sie sind jedoch hilfreiche Werkzeuge zur technischen Umsetzung von IAM. So gibt es einige standardisierte Technologien die bei der Implementierung von Identitäts- und Berechtigungsmanagement angewendet werden können. Zur konkreten Umsetzung in Organisationen gibt einige quelloffene Lösungen und von den großen Technologiekonzernen wie Microsoft, SAP, IBM, Oracle werden kommerzielle Lösungen angeboten. Im Folgenden werden einige standardisierte Technologien und Produkte vorgestellt welche bei der Umsetzung von CIAM und IAM verwendet werden.

3.4.1 Standardisierte Technologien

SAML SAML ist ein weit verbreiteter Standard zur Umsetzung von Sicherheits-Assertionen. Mit SAML wird ein XML Format definiert welches zur Authentifizierung und Authorisierung von Nutzern verwendet werden kann. Im Kontext von SAML werden verschiedene Begrifflichkeiten definiert. Hughes und Maler 2005

- Assertion - Eine Assertion über die Charakteristiken und Attribute eines Subjekts. So z.B. die Zugehörigkeit zu einer Gruppe oder der Besitz eines Attributs.
- Identity Provider (IdP) - Der Server der für die eigentliche Bearbeitung der Assertion zuständig ist. Er erhält die Anfrage und leitet die Antwort an den Service Provider weiter.
- Service Provider (SP) - Das Ziel der Authentifizierung/Authorisierung, dieser stellt eine Ressource/Service zur Verfügung.

OAuth OAuth ist ein verbreiteter Standard zur delegierten Zugriffskontrolle welcher in RFC 6749 definiert wird. OAuth ist ein Framework welches das Problem der Autorisierung Dritter löst. Somit müssen keine sensiblen Informationen wie Passwörter mit Dritten geteilt werden um ihnen Zugriff auf eine Ressource zu geben. Im Kontext des Standards werden folgende Begriffe definiert.

- Ressourcenbesitzer - Eine Entität welche die Ressource besitzt und Zugriff gewähren kann
- Ressourcenserver - Ein Server welcher die Ressource hostet und auf Anfragen mittel Zugriffstokens reagieren kann
- Klient - Eine Anwendung welcher für Ressourcen autorisiert ist und Anfragen an den Ressourcenserver senden kann
- Authorisierungsserver - Ein Server welcher Zugriffstokens im Name des Ressourcenbesitzers an den Klient ausstellen kann

Der Ablauf des Protokolls ist in Grafik Abbildung 4 abgebildet. Hardt 2012

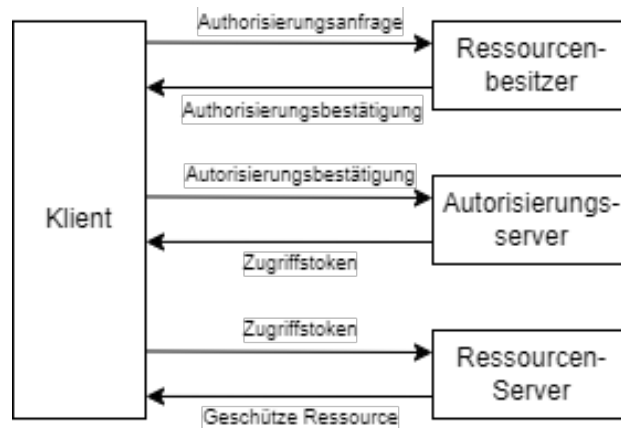


Abbildung 4: Protokoll OAuth 2.0 - Basierend auf RFC 6749

OpenID OpenID Connect (OIDC) ist ein auf OAuth 2.0 basierender Standard für föderierte Authentifizierung welches die veraltete OpenID 2.0 Spezifikation ablöst. Somit kann im Rahmen des Identitätsmanagements ein zentraler OpenID Provider (OP) über ein REST API zur Authentifizierung und SSO eingesetzt werden. Naik, Jenkins und Newell 2017

3.4.2 IAM Lösungen

Shibboleth Shibboleth ist eine quelloffene Lösung zur Umsetzung von SSO. Shibboleth basiert auf SAML und setzt daher das Prinzip der Föderierten Identität mittels IdP und SP um. Die Technologie setzt sich aus 3 Software Paketen zusammen. IdP, SP und Embedded Discovery Service. Der Embedded Discovery Service erlaubt einem SP mehrere IdP's zur Verfügung zu stellen.

IBM Security Verify IBM bietet mit dem Produkt „IBM Security Verify“ eine Cloud basierte Lösung zum Identitäts- und Berechtigungsmanagement an. Dieses Produkt bietet umfangreiche Funktionalitäten wie SSO, MFA, KI gestützte Risikobewertung von Zugriffen und Identitätsanalyse, d.h. die Analyse von Identitäten und Berechtigungen zum Zweck der Identifizierung von Abweichungen.

Microsoft Entra ID Microsoft bietet mit dem Produkt „Microsoft Entra ID“ eine Cloud basierte Lösung zum Identitäts- und Berechtigungsmana-

gement von Microsoft und drittpartei Diensten an. Dieses Produkt bietet Funktionen wie z.B. Multi-Faktor-Authentifizierung mittels Microsoft Authenticator.

SAP Cloud Identity Access Governance SAP bietet mit dem Produkt „SAP Cloud Identity Access Governence“ eine Cloud basierte Lösung zum Identitäts- und Berechtigungsmanagement an. SAP selbst schreibt dem Produkt eine intuitive Bedienung, hohe Anpassbarkeit und skalierbare Funktionen zu.

Okta Inc. Das Unternehmen Okta Inc. ist ein in den USA ansässiges Unternehmen welches sich auf IAM spezialisiert hat. Mit rund 6000 Mitarbeitern und mehr als einer Milliarde US-Dollar an Umsatz ist es ein führender Hersteller von IAM Produkten. Vom Unternehmen werden 2 Produkte angeboten. Customer Identity Cloud und Workforce Identity Cloud. Customer Identity Cloud ist eine Lösung zum Customer Identity Management, d.h. es ermöglicht die sichere Verwaltung und Authentifizierung von Kunden-Identitäten. Workforce Identity Cloud ist eine Lösung zum Unternehmensinternen Identitätsmanagement.

3.5 Erkenntnisse im Kontext von IT-GRC

- Im Rahmen von Normen wie der ISO 27001 spielt die Umsetzung von IAM eine zentrale Rolle.
- Professionelle IAM Lösungen können durch eine Vielzahl an Funktionalitäten dazu beitragen Identitäts- und Berechtigungsmanagement effizient umzusetzen.

4 Betriebliches Identitäts- und Berechtigungsmanagement

4.1 Überblick

4.2 Organisatorische Aspekte

Im Rahmen der Ausarbeitung eines IAM Konzepts im Unternehmen müssen hierbei klare Verantwortlichkeiten, Prozesse und Technologien definiert werden. Die relevanten Organisationseinheiten zum Identitäts- und Berechtigungsmanagement werden im Folgenden vorgestellt.

Führungsebene IAM fällt unter die Domäne der Informationssicherheit, benötigt jedoch gegebenenfalls umfangreiche IT Infrastruktur und Produkte. Auf der Führungsebene im Unternehmen sind daher der Chief Information Security Officer (CISO) und der Chief Information Officer (CIO) für die Umsetzung des Identitäts- und Berechtigungsmanagement verantwortlich. Azhar 2014 Baldwin, Marco Casassa Mont und Shiu 2009 Im Fall von umfangreichen Anforderungen an das System kann die Umsetzung des IAM ein ganzes Team benötigen. Mohammed, Hassan und Yusuf 2011

Helpdesk Der Helpdesk ist im Unternehmen eine zentrale Anlaufstelle für Probleme mit der Authentifizierung wie vergessener Passwörter oder fehlender Berechtigungen. So wurde bei Umfragen festgestellt dass je nach Unternehmen 10-66 % aller Helpdesk Tickets aufgrund von vergessener Passwörter erstellt werden. Ylen u. a. 2004 Tsolkas und Schmidt 2017 Ein wichtiger Aspekt hierbei ist die Einhaltung fester Prozesse welche mögliche Angriffe durch Social Engineering verhindern. Wood 2005

Personalmanagement Eine Zentrale Rolle in der Provisionierung, Änderung und Deprovisionierung von Identitäten spielt das Personalmanagement. Dieses ist für die erstmalige Erstellung der Identitäten, der Ausgabe von Authentifizierungsinformationen, der Vergabe von Rollen für rollenbasierte Zugriffskontrolle und der Deprovisionierung bei Beurlaubung und Kündigung zuständig. Young 2004 So bietet z.B. Microsoft Entra ID oder Okta Workforce Identity eine direkte Integration von HR Anwendungen in den Identitäts Lebenszyklus. Okta 2024 Billmath 2024

4.3 Technische Aspekte

Für die Umsetzung von Identitäts- und Berechtigungsmanagement im Betrieb bieten sich die Lösungen der namhaften Hersteller wie Microsoft, SAP oder Okta an. Dies sind ausgereifte Lösungen mit einer Vielzahl an Funktionalitäten die die Umsetzung des Identitäts- und Berechtigungsmanagements unterstützen. Während der traditionelle Ansatz die Nutzung von On-Premise Services war bewegt sich die IAM Industrie in Richtung von SaaS Modellen. Im Kontext von IAM werden diese Lösungen als IDaaS bezeichnet. Kunz u. a. 2014

4.4 Wirtschaftliche Aspekte

Die Signifikanz von Identitäts- und Berechtigungsmanagement in Unternehmen tiefgreifend. Es lassen sich 4 Aspekte identifizieren. Security, Produktivität, Compliance und Kundenerlebnis. M Casassa Mont u. a. 2010Azhar 2014 Diese 4 Aspekte sind im Folgenden aufgeführt.

Security Der wirtschaftliche Schaden der durch Datendiebstahl und unautorisierter Kontrolle entstehen kann ist immens. Azhar 2014 Wenn ein Mitarbeiter eine Vielzahl an Passwörtern für die unternehmensinternen/unternehmensexternen Dienste verwalten muss kann dies zur unsachgemäßen Handhabung führen - so z.B. Notizen mit Passwörtern oder die Verwendung von schwachen Passwörtern, dies erhöht die Wahrscheinlichkeit von Sicherheitsrisiken. Haag und Spruit 2012 Azhar 2014 Im Jahr 2017 fiel Deloitte einem Cyberangriff zum Opfer. Hierbei wurden Nutzernamen, Passwörter, IP Adressen und sensible Unternehmensinformationen von 244.000 Mitarbeitern und Kunden geklaut. Grund für den Cyberangriff war ein Administratoraccount ohne Zugriffsbeschränkungen welcher nur mittels Passwort, ohne MFA geschützt war. Deloitte 2017 Mittels fest definierter Prozesse des Identity Management Life Cycles und Audit dieses können Risiken für ähnliche Angriffe minimiert werden.

Produktivität Im vorherigen Abschnitt wurde die sicherheitstechnische Signifikanz von Identitäts- und Berechtigungsmanagement aufgezeigt. Dies kann jedoch einen negativen Einfluss auf die Produktivität von Mitarbeitern haben. So führt z.B. die Verwendung von mehreren verschiedenen Systemen, alle mit unterschiedlichen Authentifizierungsverfahren dazu dass Mitarbeiter

verschiedene Passwörter verwalten müssen oder sich in jedem System separat authentifizieren müssen. Radha und Reddy 2012 Haag und Spruit 2012 Ein weiterer Aspekt sind vergessene Passwörter mit Unterbrechungen im Arbeitsablauf und hohem Helpdesk aufwand. Mit der Anwendung von SSO Verfahren lässt sich dieser Aufwand auf ein Minimum reduzieren. Thakur und Gaikwad 2015 Während die Umsetzung des Principle of Least Privilege wünschenswert ist können schlecht konfigurierte Zugriffsberechtigungen dazu führen dass Mitarbeiter ihre Arbeit unterbrechen müssen um neue Rechte anzufordern. Dies kann unter Umständen zu teuren Verzögerungen im direkten Arbeitsablauf administrativer oder operativer Aufgaben führen. Weishäupl u. a. 2015

Kundenerlebnis Im Kontext des Customer IAM führen ungeeignete IAM Lösungen zu erhöhter Komplexität für den Nutzer. Eine strikte Umsetzung von starken Passwörtern oder die Nutzung einer weiteren MFA-App kann für den Kunden abschreckend sein. Somit steigt der Kunde möglicherweise zur Konkurrenz um. Azhar 2014 Durch das Anbieten von SSO mittels externer Dienste lässt sich die Komplexität und das Risiko von Sicherheitsproblemen reduzieren.

Wettbewerbsvorteil durch Zertifizierungen Zertifizierungen mit Sicherheitsstandards wie der ISO 27001 können zu einem Wettbewerbsvorteil führen denn diese sind ein Indikator für Qualität. Dobrin u. a. 2015 Somit kann die Umsetzung von Identitäts- und Berechtigungsmanagement im Rahmen einer ISO 27001 Zertifizierung zu einem Wettbewerbsvorteil führen.

Compliance

EuroSOX Die Richtlinie 2006/43/EG, durch den direkten Bezug zum Sarbanes Oxley Act auch EuroSOX genannt fordert im Rahmen des Internen Kontrollsystems (IKS) nach einer Berechtigungsvergabe und Funktionstrennung im Unternehmen. Dies stellt eine direkte Forderung für Identitäts- und Berechtigungsmanagement dar. Conta 2017

KonTraG Das KonTraG fordert Unternehmen auf ein Risikomanagementsystem zu implementieren. Unauthorisierter Zugriff auf sensible Daten und Geschäftsprozesse kann in diesem Kontext als Risiko aufgefasst werden.

D.h. es besteht eine indirekte Forderung nach Identitäts- und Berechtigungsmanagement. Conta 2017

BDSG Im BDSG nimmt Identitäts- und Berechtigungsmanagement eine zentrale Rolle ein.

- Zutrittskontrolle, Zugriffskontrolle: Systeme die personenbezogene Daten verarbeiten müssen vor unauthorisiertem Zutritt und Zugriff geschützt werden. Conta 2017 Dies stellt eine direkte Forderung für physische und logische Berechtigungskontrollen dar.
- Weitergabekontrolle: Beim Transport von personenbezogenen Daten die Vertraulichkeit und Integrität der Daten gewährleistet wird und dass jegliche Transaktionen protokolliert werden müssen. Conta 2017 Dies stellt eine direkte Forderung für Audit-Trails und Berechtigungskontrollen dar.
- Eingabekontrolle: Bei der Erfassung von personenbezogenen Daten muss die Nachvollziehbarkeit des Ursprungs gewährleistet sein. Conta 2017 Dies stellt eine direkte Forderung für Audit-Trails dar.

EU-DSGVO Die DSGVO stellt verschiedenste Forderungen für die sichere Erhebung, Speicherung und Verarbeitung von personenbezogener Daten. Hindle 2020

- Artikel 5 - Grundsätze für die Verarbeitung personenbezogener Daten - Paragraph 1.f: Die Integrität und Vertraulichkeit personenbezogener Daten muss gewährleistet sein. Union 2016 Somit müssen geeignete Verfahren zur Zutritts und Zugriffskontrolle vorhanden sein.
- Artikel 15 - Auskunftsrecht der betroffenen Person - Paragraph 3: Das betroffene Person über die Daten erhoben wurde hat das Recht Auskunft über alle personenbezogenen Daten anzufordern. Union 2016 Hierbei sind geeignete Prozesse im Rahmen des Identitätsmanagements zu definieren. Diese müssen durch geeignete Authentifizierungsverfahren geschützt werden um die Vertraulichkeit der Weitergabe zu gewährleisten.
- Artikel 17 - Recht auf Löschung - Paragraph 1: Die betroffene Person hat das Recht eine Forderung für die unverzügliche Löschung der Daten einzureichen. Union 2016 Hierbei sind geeignete Prozesse im Rahmen des Identitätsmanagements zu definieren.

4.5 Erkenntnisse im Kontext von IT-GRC

- Die Umsetzung von IAM kann kostspielig sein denn das Management und die eingesetzten Technologien sind teuer. Rechtlichen Vorgaben sind jedoch nicht optional und die Risiken von fehlendem IAM können enorm sein.
- Es gibt eine Vielzahl rechtlicher Vorgaben welche die Umsetzung von Identitäts- und Berechtigungsmanagement fordern. So z.B. das EuroS-OX, KonTraG, BDSG und die EU-DSGVO
- Die sorgfältige Umsetzung von Identitäts- und Berechtigungsmanagement im Rahmen eines Informationssicherheitsmanagementsystems spielt eine zentrale Rolle im Risikomanagement

5 Fazit

5.1 Zusammenfassung

5.2 Beantwortung der Forschungsfragen

Identität und Identitätsmanagement Eine (digitale) Identität ist eine Menge von Attributen und Rollen, inklusive Bezeichner und Zugangsdaten zur Autorisierung. So kann eine Identität eine Person, ein IT-System oder eine Anwendung darstellen. Eine Identität kann einer Entität, also einer Person oder einer Organisation zugeordnet werden. Das Identitätsmanagement ist zuständig für die Festlegung von Prozessen zur Verwaltung, Authentifizierung und Überwachung von Identitäten.

Berechtigung und Berechtigungsmanagement Eine Berechtigung ist eine Kombination aus zu berechtigender Ressource und zu berechtigender Operation auf diese Ressource. Berechtigungsmanagement bezeichnet die Prozesse für die Zuweisung, Kontrolle, Überwachung und Entzug von Berechtigungen sowie der Überwachung dieser Prozesse.

Welche Standards, Methoden, Technologien und Tools lassen sich differenzieren? Die ISO 27001 Norm in Kombination mit dem IT-Grundschutz

des BSI's stellt einen Goldstandard in der Informationssicherheit in Organisationen dar. Ein wichtiger Aspekt einer ISO 27001 Zertifizierung ist die Zugriffskontrolle. Es haben sich einige standardisierte Verfahren zur Umsetzung von Identitäts- und Berechtigungsmanagement etabliert, so z.B. SAML, OAuth, OpenID Connect. Es gibt eine Vielzahl an Anbietern welche IAM Lösungen anbieten. Beispiele für große Hersteller sind Microsoft, IBM, SAP und Okta.

Welche Aufgaben und Prozesse sind im Kontext von Identitäts- und Berechtigungsmanagement zu bearbeiten? Die grundlegenden Aufgaben und Prozesse des Identitäts- und Berechtigungsmanagements sind:

- Provisionierung, Änderung und Deprovisionierung von digitalen Identitäten und Berechtigungen
- Technische Umsetzung der Infrastruktur zur Speicherung der relevanten Informationen, der Authentifizierung und der Autorisierung
- Identifikation von rechtlichen Aspekten und Standards, Planung von Prozessen zur Einhaltung dieser
- Auditierung aller Prozesse zur Identifikation von Abweichungen und Speicherung von Informationen im Rahmen der Rückverfolgbarkeit von Transaktionen

Welche betrieblichen Anwendungsfälle zeigen die Bedeutung des Identitäts und Berechtigungsmanagements auf?

Wie wird das Identitäts und Berechtigungsmanagement im Kontext der Sicherheit in der Informationstechnik eingesetzt? Das Identitäts- und Berechtigungsmanagement wird eingesetzt um Zugriffe auf schützenswerte Ressourcen einzuschränken. Dies geschieht durch geeignete Authentifizierungs und Autorisierungsverfahren.

Zuständigkeit für Identitäts- und Berechtigungsmanagement Für die Planung und Umsetzung der Prozessen des Identitäts- und Berechtigungsmanagements ist im Unternehmen der CIO verantwortlich. Dieser wird ggf. durch den CISO unterstützt denn Identitäts- und Berechtigungsmanagement

ist ein sicherheitskritischer Prozess. Operativ involviert sind die Personalverwaltung und der Helpdesk. Die Personalverwaltung ist zuständig für die Erstellung, Änderung und Löschung von Identitäten und Rollen. Der Helpdesk ist die Anlaufstelle für Probleme bei der Nutzung von Identitäts- und Berechtigungsmanagement-Systemen und bei Incidents.

6 Eidesstattliche Versicherung

Literaturverzeichnis

- Ylen, Mikko u. a. (2004). "Centralized password management in a global enterprise". Magisterarb.
- Young, Dale (2004). "Human Resources have a vital role to play within employee identity and access management". In: *Network Security* 2004.11, S. 5–7. ISSN: 1353-4858. URL: <https://www.sciencedirect.com/science/article/pii/S1353485804001540>.
- Hughes, John und Eve Maler (2005). "Security assertion markup language (saml) v2. 0 technical overview". In: *OASIS SSTC Working Draft sstc-saml-tech-overview-2.0-draft-08* 13, S. 12.
- Wood, Peter (2005). "Implementing identity management security-an ethical hacker's view". In: *Network Security* 2005.9, S. 12–15.
- Baldwin, Adrian, Marco Casassa Mont und Simon Shiu (2009). "Using modelling and simulation for policy decision support in identity management". In: *2009 IEEE International Symposium on Policies for Distributed Systems and Networks*. IEEE, S. 17–24.
- Bertino, Elisa und Kenji Takahashi (2010). *Identity management: Concepts, technologies, and systems*. Artech House.
- Mont, M Casassa u. a. (2010). "Economics of identity and access management: a case study on enterprise business services". In: *HP Laboratories, Technical Report HPL-2010-11*.
- Mohammed, Ishaq Azhar, Abubakar Hassan und DM Yusuf (2011). "Identity and access management system: a web-based approach for an enterprise". In: *International Journal of Advanced and Innovative Research* 1.4, S. 1–7.
- Haag, Peter und Marco Spruit (2012). "Selecting and implementing Identity and Access Management technologies: The IAM Services Assessment Model". In: *Digital Identity and Access Management: Technologies and Frameworks*. IGI Global, S. 348–365.
- Radha, V und D Hitha Reddy (2012). "A survey on single sign-on techniques". In: *Procedia Technology* 4, S. 134–139.
- Azhar, Ishaq (2014). "Economics of Identity and Access Management: Providing decision support for investments". In: *Ishaq Azhar Mohammed. (2014). Economics of Identity and Access Management: Providing decision support for investments. International Journal of Managment, IT and Engineering (IJMIE)* 4.2, S. 540–549.

- Kunz, Michael u. a. (2014). “Analyzing Recent Trends in Enterprise Identity Management”. In: *2014 25th International Workshop on Database and Expert Systems Applications*, S. 273–277.
- Dobrin, Cosmin u. a. (2015). “Quality: a determinant factor of competitiveness—the evolution of iso certifications for management systems”. In: *Proceedings of the International Management Conference*. Bd. 9. 1, S. 1062–1073.
- Thakur, Manav A und Rahul Gaikwad (2015). “User identity and access management trends in IT infrastructure—an overview”. In: *2015 International Conference on Pervasive Computing (ICPC)*. IEEE, S. 1–4.
- Weishäupl, Eva u. a. (2015). “Towards an economic approach to identity and access management systems using decision theory”. In.
- Conta, Daniel (2017). “Leitfaden eines mandantenunabhängigen Identity Access Management”. Diss. Hochschule für angewandte Wissenschaften Hamburg.
- Mohammed, Ishaq Azhar (2017). “Systematic review of identity access management in information security”. In: *International Journal of Innovations in Engineering Research and Technology* 4.7, S. 1–7.
- Naik, Nitin, Paul Jenkins und David Newell (2017). “Choice of suitable identity and access management standards for mobile computing and communication”. In: *2017 24th International Conference on Telecommunications (ICT)*. IEEE, S. 1–6.
- Tsolkas, Alexander und Klaus Schmidt (2017). “Rollen und Berechtigungskonzepte: Identity- und Access-Management im Unternehmen”. In: Wiesbaden: Springer Fachmedien Wiesbaden. ISBN: 978-3-658-17987-8. URL: https://doi.org/10.1007/978-3-658-17987-8_7.
- Hindle, Andrew (März 2020). *Impact of GDPR on identity and Access Management*. URL: <https://bok.idpro.org/article/id/24/print/>.
- Kersten, Heinrich u. a. (2020). “IT-Sicherheitsmanagement nach der neuen ISO 27001”. In: *ISMS, Risiken, Kennziffern, Controls* 2.
- Ghaffari, Fariba u. a. (2022). “Identity and access management using distributed ledger technology: A survey”. In: *International Journal of Network Management* 32.2, e2180.
- Liveretos, Anastasios und Ivo Draganov (2022). “Customer Identity and Access Management (CIAM): An overview of the main technology vendors”. In: *International Journal of Economics and Management Systems* 7.

Quellenverzeichnis

- Hardt, Dick (2012). *RFC 6749: The oauth 2.0 authorization framework*. URL: <https://datatracker.ietf.org/doc/html/rfc6749> (besucht am 28.05.2024).
- Union, Europäische (Mai 2016). URL: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE> (besucht am 28.05.2024).
- BSI (2017a). URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (besucht am 28.05.2024).
- (Nov. 2017b). URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.html (besucht am 28.05.2024).
- Deloitte (2017). URL: <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-FactsSheetforGlobalWebsite-cyber-attack.pdf> (besucht am 28.05.2024).
- BSI (Dez. 2021a). URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium/Zuordnung_ISO_und_IT_Grundschutz.html (besucht am 28.05.2024).
- (2021b). *ORP.4: Identitäts- und Berechtigungsmanagement*. 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).
- (2022). URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2022/Umsetzungshinweis_zum_Baustein_ORP_4_Identitaets_und_Berechtigungsmanagement.pdf?__blob=publicationFile&v=2 (besucht am 28.05.2024).
- (Sep. 2023a). URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompodium/it-grundschutz-kompodium_node.html (besucht am 28.05.2024).
- (Sep. 2023b). URL: <https://www.bsi.bund.de/dok/6604686> (besucht am 28.05.2024).

- ISO (2023). *ISO/IEC 24760-1:2019 IT Security and Privacy - A framework for identity management 2023*. URL: <https://www.iso.org/standard/77582.html> (besucht am 28.05.2024).
- Billmath (Apr. 2024). *Was ist die Personalgesteuerte Bereitstellung mit microsoft entra ID? - microsoft entra ID*. URL: <https://learn.microsoft.com/de-de/entra/identity/app-provisioning/what-is-hr-driven-provisioning> (besucht am 28.05.2024).
- Okta (2024). *HR-Driven IT Provisioning*. URL: <https://www.okta.com/resources/whitepaper/olm-technical-whitepaper-hr-driven-it-provisioning/> (besucht am 28.05.2024).

Abbildungsverzeichnis

1	Digitale Identität - In Anlehnung an Grafik 2.1 aus Identity Management Concepts, Technologies, and Systems von Elisa Bertino und Kenji Takahashi	5
2	Illustration der Zugriffssteuerung im Rahmen eines IAM Systems - In Anlehnung an Ghaffari u. a. 2022 Abbildung 1	8
3	Identity Life Cycle - In Anlehnung an Identity Management Concepts, Technologies, and Systems von Elisa Bertino und Kenji Takahashi	10
4	Protokoll OAuth 2.0 - Basierend auf RFC 6749	14