CANCOM

FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachhochschule Aachen

Fakultät
Technomathematik und Medizintechnik

Studium
Angewandte Mathematik und Informatik B.Sc.

Gegenüberstellung von OIDC basierten Single-Sign-On-Technologien zur Modernisierung eines Dienstes unter Berücksichtigung von High-Availability, MFA und einfacher Integration von externen Service-Providern

---

Seminararbeit
Christopher-Jannik Mauthe
Matrikelnummer: 3533192

Aachen, 19. Dezember 2023

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Aachen, am ....

(Christopher-Jannik Mauthe)

Abstract

Diese Arbeit untersucht die Leistungsfähigkeit und Anwendbarkeit der Open-Source-Single Sign-On (SSO)-Technologien Keycloak und Authentik. Keycloak zeichnet sich durch seine High-Availability und Sicherheitsmerkmale aus, während Authentik durch seine Integrations- und Benutzerfreundlichkeitsmerkmale hervorsticht. Beide Technologien unterstützen Multi-Faktor Authentifizierung (MFA) und ermöglichen die Integration von externen Service-Providern. Die Analyse zeigt, dass Keycloak aufgrund seiner höheren Punktzahl in High-Availability und Sicherheit bevorzugt wird, während Authentik in Bezug auf Integration und Benutzerfreundlichkeit besser abschneidet. Es ist jedoch wichtig zu beachten, dass die Wahl zwischen den beiden Technologien von den spezifischen Anforderungen und Prioritäten des Benutzers abhängt.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

2FA	Zwei-Faktor-Authentifizierung
FIM	Federal Identity Management
IAM	Identity und Access Management
IdP	Identity Provider
JWT	JSON Web Token
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Faktor Authentifizierung
OAuth	Open Authorization
OIDC	OpenID Connect
OTP	One-Time Password
SAML	Security Assertion Markup Language
SP	Service-Provider
SSO	Single Sign-On
TOTP	Time-based One-Time Password
WebAuthn	Web Authentication

Kapitel 1

Einleitung

In einer immer stärker vernetzten Welt ist die effektive und sichere Verwaltung von Nutzeridentitäten und Zugriffsrechten eine zentrale Herausforderung für moderne IT-Systeme. Dies gilt insbesondere für Dienste, die von einer Vielzahl von externen Service-Providern (SPs) genutzt werden.

1.1 Hintergrund und Motivation

Das Ziel dieser Arbeit ist es, einen Vergleich der beiden OpenID Connect (OIDC)-basierten SSO-Technologien Keycloak und Authentik zu schaffen und ihre Eignung für die Modernisierung des laufenden Dienstes zu bewerten. Dabei sollen insbesondere die Aspekte High-Availability, MFA und die Integration von externen SPs berücksichtigt werden. Die wissenschaftliche Relevanz der Arbeit ergibt sich aus der Tatsache, dass trotz der zunehmenden Verbreitung von OIDC-basierten SSO-Technologien noch zahlreiche Fragen hinsichtlich ihrer optimalen Anwendung und Weiterentwicklung offen sind. Durch eine systematische Untersuchung und Bewertung der verschiedenen Technologien kann diese Arbeit einen wichtigen Beitrag zur Beantwortung dieser Fragen leisten.

1.2 Forschungsfragen

Die Forschungsfragen, die in dieser Arbeit behandelt werden, sind von entscheidender Bedeutung für die Zukunftsfähigkeit des Dienstes und seine Fähigkeit, den steigenden Anforderungen an Sicherheit, Verfügbarkeit und Interoperabilität gerecht zu werden.

1.2.1 Wie kann die SSO-Technologie mit OIDC zur Modernisierung eines Dienstes beitragen?

Diese Forschungsfrage bildet den Hauptaspekt der Arbeit und zielt darauf ab, zu zeigen, wie der Übergang von SimpleSAMLphp zu OIDC-basierten SSO-Technologien wie Keycloak und Authentik dazu beitragen kann, den Dienst zu modernisieren. Die Arbeit wird die Vorteile von OIDC im Vergleich zu traditionellen SSO-Methoden aufzeigen.

1.2.2 Wie kann die Implementierung von High-Availability und MFA in OIDC-basierten SSO-Systemen erreicht werden?

Diese Forschungsfrage konzentriert sich auf die Erhöhung der Sicherheit und Verfügbarkeit des Dienstes. Die Arbeit wird Methoden und bewährte Verfahren zur Implementierung von High-Availability und MFA in OIDC-basierten SSO-Systemen untersuchen.

1.2.3 Wie können externe SP einfach in ein OIDC-basiertes SSO-System integriert werden?

Diese Forschungsfrage adressiert die Notwendigkeit, die Interoperabilität und die Fähigkeit zur Integration mit externen Dienstleistern zu verbessern. Die Arbeit wird aufzeigen, wie OIDC-basierte SSO-Systeme wie Keycloak und Authentik die Integration von externen SPs erleichtern können, und praktische Ansätze für eine reibungslose Integration bereitstellen.

1.3 Methodik

Um die Forschungsfragen beantworten zu können, werden im Ramen dieser Arbeit folgende Ansätze verfolgt. Die Methodik umfasst eine Kombination aus Literaturrecherche, technischer Analyse, Nutzwertanalyse und Interviews, um ein umfassendes Verständnis der Themen zu entwickeln und die Fragen zu beantworten. Die Kombination dieser methodischen Ansätze ermöglicht eine Untersuchung der Forschungsfragen und trägt dazu bei, klar definierte und fundierte Aussagen zu treffen.

1.3.1 Literaturrecherche und technische Analyse

Die Literaturrecherche bildet den ersten Schritt in der methodischen Vorgehensweise. Hierbei wird eine breite Palette von Quellen, einschließlich wissenschaftlicher Artikel, Studien und technischer Dokumentationen, untersucht. Dies ermöglicht ein solides Fundament für die Seminararbeit zu schaffen und das bestehende Wissen über OIDC, SSO, High-Availability, MFA und die Integration von externen SPs zu erfassen.

1.3.2 Nutzwertanalyse

Die Nutzwertanalyse bildet den nächsten Schritt der Methodik. Basierend auf den Ergebnissen der technischen Analyse und unter Berücksichtigung der Unternehmensanforderungen wird eine umfassende Nutzwertanalyse durchgeführt. Dabei fließen Aspekte Unternehmenskompatibilität, Benutzerfreundlichkeit und Support in die Bewertung ein.

Kapitel 2

Grundlagen

2.1 Definition der zentralen Begriffe

In dieser Sektion werden die Schlüsselbegriffe definiert, die für das Verständnis der vorliegenden Seminararbeit nötig sind.

2.1.1 Single Sign-On

SSO ist ein zentrales Konzept im Bereich der Authentifizierung und Sicherheit in Informationssystemen. [6, Abstract] Es bezieht sich auf die Fähigkeit eines Benutzers, sich einmalig zu authentifizieren und anschließend auf mehrere Dienste oder Anwendungen zuzugreifen, ohne sich erneut anzumelden. Dieses Konzept bietet zahlreiche Vorteile, darunter eine verbesserte Benutzerfreundlichkeit, erhöhte Sicherheit und eine effizientere Verwaltung von Zugriffsrechten.

Vorteile von SSO

SSO ist in vielen Unternehmen und Organisationen weit verbreitet. Dies zeigt sich in den zahlreichen Vorteilen, die es bietet:

Benutzerfreundlichkeit: SSO reduziert die Notwendigkeit für Benutzer, sich bei jedem einzelnen Dienst oder jeder Anwendung separat anzumelden. Dies führt zu einer verbesserten Benutzererfahrung und spart Zeit.

Effizienz: Die einmalige Anmeldung vereinfacht die Verwaltung von Zugriffsrechten und Sicherheit, da Benutzerkonten und Kennwörter an einer zentralen Stelle verwaltet werden können.

Sicherheit: SSO ermöglicht eine zentralisierte Überwachung und Kontrolle der Anmeldungen, erleichtert die Durchsetzung von Sicherheitsrichtlinien und reduziert das Risiko auf Sicherheitslücken. Dies wird erreicht durch die Einhaltung des Prinzips der Separation of Concerns [2], das die Verantwortung für die Benutzerauthentifizierung auf ein einziges, zentrales System verlagert.

Reduzierung von Passwort-Fatigue: Benutzer müssen sich weniger Kennwörter merken, was die Wahrscheinlichkeit von unsicheren Praktiken wie das Wiederverwenden von Kennwörtern reduziert.

Funktionsweise von SSO

Die Funktionsweise von SSO basiert auf der Verwendung von Authentifizierungstoken. Ein Benutzer authentifiziert sich bei der ersten Anmeldung an einem Identity Provider (IdP), der die Identität des Benutzers überprüft. Nach erfolgreicher Authentifizierung generiert der IdP einen Token, der dem Benutzer zugewiesen wird. Dieser Token wird bei weiteren Zugriffen auf Dienste oder Anwendungen anstelle der wiederholten Anmeldedaten verwendet.

Arten von SSO

SSO kann auf verschiedene Arten implementiert werden, je nach den spezifischen Anforderungen des Systems und den Sicherheitsrichtlinien. Die gängigsten Arten von SSO sind:

SAML-basiertes SSO: Security Assertion Markup Language (SAML) ist ein Protokoll, welches Anmeldeinformationen in das XML-Format einbettet und dieses zur Datenübertragung verwendet. Der generierte SAML-Token, der Daten des Benutzers enthält, ist eine der verbreitetsten Varianten des SSO.

OAuth-basiertes SSO: Open Authorization (OAuth) wird hier als Vereinfachung für OAuth 2.0 benutzt. Dies ist der Nachfolger von OAuth 1.0 und ist schneller und weniger kompliziert als seine ältere Variante, obwohl es mehr Prozessschritte enthält. Es ist ein Protokoll, das für die Autorisierung verwendet wird. Es ermöglicht es einer Anwendung, auf Ressourcen eines anderen Dienstes zuzugreifen, ohne dass die Benutzer ihre Anmeldeinformationen an diese Anwendung weitergeben müssen. Es erstellt einen Zugriffstoken, der an den Ressourcenserver gesendet wird, und nach erfolgreicher Prüfung des Tokens gewährt der Ressourcenserver Zugriff.

OIDC-basiertes SSO: OIDC ist eine Erweiterung des OAuth 2.0 Protokolls. Es dient dazu, die Identität von Endnutzern zu überprüfen, die sich bei einem Autorisierungsserver anmelden. Außerdem liefert es grundlegende Profilinformationen über den Endbenutzer auf eine einfache und unkomplizierte Weise.

[5, Types of SSO]

Sicherheitsaspekte von SSO

Obwohl SSO zahlreiche Vorteile bietet, sind auch Sicherheitsaspekte zu berücksichtigen. SSO erfordert ein hohes Maß an Sicherheit, da ein Kompromittieren des SSO-Systems den Zugriff auf alle verknüpften Dienste ermöglichen könnte. Daher ist die sichere Implementierung von SSO, die Verwendung von Verschlüsselung und die Überwachung von Anmeldeaktivitäten von entscheidender Bedeutung, um Sicherheitsverletzungen zu verhindern.

Die Integration von MFA in SSO-Systeme ist eine gängige Praxis, um die Sicherheit weiter zu erhöhen. MFA erfordert zusätzliche Sicherheitsüberprüfungen neben Benutzername und Passwort, wie beispielsweise Fingerabdruckerkennung oder Einmalpasswörter.

2.1.2 Multi-Faktor Authentifizierung

MFA, auch als Zwei-Faktor-Authentifizierung (2FA) bezeichnet, ist eine Sicherheitsmethode, bei der ein Benutzer nicht nur einen einzelnen Faktor, typischerweise ein Passwort, zur Authentifizierung verwendet, sondern mindestens zwei verschiedene Faktoren. Das erhöht die Sicherheit, da ein Angreifer nicht nur das Passwort, sondern auch den Zugang zu einem weiteren, unabhängigen Faktor kennen muss um sich zu authentifizieren.

Die Faktoren von MFA

MFA basiert auf der Verwendung mehrerer Authentifizierungsmechanismen, die in der Regel in drei Kategorien unterteilt werden:

Wissensfaktoren (Something You Know): Dies umfasst traditionelle Kennwort- oder PIN-basierte Authentifizierung, bei der der Benutzer etwas wissen muss, um sich zu authentifizieren.

Besitzfaktoren (Something You Have): Diese Kategorie bezieht sich auf physische Gegenstände oder Geräte, die der Benutzer besitzt und zur Authentifizierung verwendet, wie Smartcards, Mobiltelefone oder Hardware-Token.

Inhärenz-Faktoren (Something You Are): Dieser Faktor bezieht sich auf biometrische Merkmale des Benutzers, wie Fingerabdrücke, Gesichtserkennung oder Retina-Scans.

[3, 1. Introduction]

Funktionsweise von MFA

MFA erfordert, dass der Benutzer mindestens zwei der oben genannten Faktoren bereitstellt, um sich erfolgreich zu authentifizieren. Dies kann auf verschiedene Arten implementiert werden, basierend auf den Anforderungen und den verfügbaren Technologien. Die am häufigsten verwendeten Implementierungen von MFA umfassen:

Authentifizierungs-Apps: Der Benutzer verwendet eine spezielle App, beispielsweise auf seinem Smartphone, um Einmal-Codes zu generieren oder Push-Benachrichtigungen für die Authentifizierung zu erhalten.

Biometrische Authentifizierung: Der Benutzer verwendet biometrische Merkmale wie Fingerabdrücke oder Gesichtserkennung in Verbindung mit seinem Passwort.

Hardware-Token: Der Benutzer hat einen physischen Hardware-Token, der zur Generierung von Einmal-Codes verwendet wird.

[3, 2. State-of-the-Art and Potential MFA Sources]

Bedeutung von MFA

MFA spielt eine entscheidende Rolle in der Sicherheit von Informationssystemen. Es bietet einen zusätzlichen Schutz, der die Wahrscheinlichkeit von unbefugten Zugriffen verringert. Dies ist besonders relevant in Umgebungen, in denen sensible Daten oder geschäftskritische Anwendungen geschützt werden müssen. Die Kombination von MFA mit SSO kann die Sicherheit weiter erhöhen, da sie sowohl den Benutzerkomfort als auch die Sicherheit maximiert.

Herausforderungen bei der Implementierung von MFA

Die Implementierung von MFA kann mit einigen Herausforderungen verbunden sein, darunter die Kompatibilität mit verschiedenen Diensten und Anwendungen sicherzustellen. Es erfordert auch eine sorgfältige Planung und die Auswahl der am besten geeigneten MFA-Methoden, um die Sicherheitsanforderungen zu erfüllen.

2.1.3 OpenID Connect

OpenID Connect (OIDC) ist eine Identitätsschicht auf OAuth 2.0, die die Authentifizierung von Benutzern ermöglicht. Es baut auf dem OAuth 2.0 Protokoll auf und erweitert dessen Funktionalität, indem es die Authentifizierung des Benutzers hinzufügt. Dadurch können OIDC spezifische Berechtigungen für jeden Benutzer in der Ziel-App zugewiesen werden. Bei dieser Methode wird ein Token generiert, das die Anmeldedaten des Benutzers enthält. Dieser Token wird bei weiteren Zugriffen auf Dienste oder Anwendungen anstelle der wiederholten Anmeldung verwendet. Darüber hinaus bietet OIDC zusätzliche Daten, die es dem Client ermöglichen, zu sehen, wer sich eingeloggt hat und mit welchem Zugriffslevel, was die Benutzerverwaltung erleichtert. [13]

Vorteile von OIDC

OIDC bietet mehrere Vorteile, die es zu einer attraktiven Wahl für die Authentifizierung machen:

Benutzerfreundlichkeit: OIDC vereinfacht den Authentifizierungsprozess. Es ermöglicht den Benutzern, sich einmal anzumelden und auf mehrere Anwendungen zuzugreifen.

Sicherheit: OIDC verwendet Industriestandard-Sicherheitsmechanismen wie JSON Web Tokens (JWTs) für die Übertragung von Identitätsinformationen. Dies gewährleistet eine sichere Kommunikation zwischen dem OIDC-Anbieter und der Anwendung und reduziert das Risiko unbefugter Zugriffe.

Effizienz: Es wird nur eine zentrale Authentifizierungsinstanz benötigt, der von allen verwalteten Diensten vertraut wird. Dies vereinfacht das Sicherheitsmodell in dem Anwendungssystem.

Funktionsweise von OIDC

Die Funktionsweise von OIDC basiert auf der Verwendung von Authentifizierungstoken. Ein Benutzer authentifiziert sich bei der ersten Anmeldung an einem IdP, der die Identität des Benutzers überprüft. Nach erfolgreicher Authentifizierung generiert der IdP ein Token, das dem Benutzer zugewiesen wird. Dieser Token wird bei weiteren Zugriffen auf Dienste oder Anwendungen anstelle der wiederholten Anmeldung verwendet.

Arten von OIDC

OIDC kann auf verschiedene Arten implementiert werden, je nach den spezifischen Anforderungen des Systems und den Sicherheitsrichtlinien. Einige der gängigsten Arten von OIDC sind:

Autorisierungscode-Fluss: Bei dieser Methode erhält der Client nach erfolgreicher Authentifizierung des Benutzers einen Autorisierungscode vom IdP. Dieser Code wird dann gegen ein Access Token und ein Refresh Token ausgetauscht.

Impliziter Fluss: Hierbei wird das Access Token direkt nach der Authentifizierung des Benutzers an den Client zurückgegeben. Dieser Fluss wird oft in mobilen oder Web-Anwendungen verwendet, in denen ein Client-Secret nicht sicher gespeichert werden kann.

Hybrid-Fluss: Dies ist eine Kombination aus dem Autorisierungscode- und dem impliziten Fluss. Hier erhält der Client sowohl einen Autorisierungscode als auch ein Access Token direkt nach der Authentifizierung des Benutzers.

[13, OIDC-Flows]

Die Wahl der Implementierung hängt von den spezifischen Anforderungen des Systems und den Sicherheitsrichtlinien ab. Es ist wichtig zu beachten, dass unabhängig von der gewählten Implementierung, die sichere Implementierung von OIDC, die Verwendung von Verschlüsselung und die Überwachung von Anmeldeaktivitäten von entscheidender Bedeutung sind, um Sicherheitsverletzungen zu verhindern.

2.1.4 High-Availability

High-Availability ist ein Konzept in der Systemadministration und Anwendungsentwicklung, das sich darauf konzentriert, die Ausfallzeiten eines Systems zu minimieren und die Verfügbarkeit von Anwendungen und Diensten zu maximieren. Ein hochverfügbares System ist so konzipiert, dass es kontinuierlich läuft, selbst wenn einzelne Komponenten ausfallen.

Grundprinzipien der High-Availability

Die Hauptprinzipien der High-Availability sind Redundanz und Fehlertoleranz.

Redundanz bezieht sich auf die Existenz von mehreren Komponenten, die dieselbe Funktion erfüllen. Wenn eine Komponente ausfällt, kann eine andere Komponente ihre Funktion übernehmen, um den Dienst aufrechtzuerhalten.

Fehlertoleranz ist die Fähigkeit eines Systems, auch bei Ausfall einer oder mehrerer Komponenten weiterhin zu funktionieren. Dies wird oft durch den Einsatz von Redundanz und der Fähigkeit des Systems, automatisch auf Ausfälle zu reagieren, erreicht.

Die Kombination dieser beiden Prinzipien führt dazu, dass hochverfügbare Systeme in der Lage sind, Ausfälle zu tolerieren und gleichzeitig die Dienste für die Benutzer verfügbar zu halten.

Umsetzung von High-Availability

Die Umsetzung von High-Availability erfordert eine sorgfältige Planung und Implementierung. Einige der Techniken und Methoden, die zur Erreichung der High-Availability verwendet werden, umfassen:

Redundante Hardware: Dies kann redundante Server, Speichergeräte und Netzwerkkomponenten umfassen. Durch den Einsatz redundanter Hardware kann das System weiterhin funktionieren, auch wenn eine einzelne Komponente ausfällt.

Clustering: Ein Cluster ist eine Gruppe von Servern, die zusammenarbeiten, um einen Dienst bereitzustellen. Wenn ein Server in einem Cluster ausfällt, kann ein anderer Server seine Aufgaben übernehmen.

Load Balancing: Load Balancing verteilt den Netzwerkverkehr auf mehrere Server, um sicherzustellen, dass kein einzelner Server überlastet wird. Dies kann dazu beitragen, die Verfügbarkeit zu erhöhen und die Leistung zu verbessern.

Datenreplikation: Datenreplikation bezieht sich auf das Kopieren von Daten von einem Ort zu einem anderen, um sicherzustellen, dass die Daten auch bei einem Ausfall verfügbar sind.

Monitoring und automatische Wiederherstellung: Durch das ständige Überwachen des Systemzustands und das automatische Wiederherstellen von Diensten oder Servern bei einem Ausfall kann die Verfügbarkeit erhöht werden.

Bedeutung von High-Availability

Die Bedeutung von High-Availability kann nicht hoch genug eingeschätzt werden, insbesondere in Umgebungen, in denen Ausfallzeiten erhebliche finanzielle Verluste oder negative Auswirkungen auf das Geschäft haben können. Die Aufrechterhaltung der Verfügbarkeit von Diensten und Anwendungen ermöglicht es Unternehmen, sicherzustellen, dass ihre Geschäftsprozesse reibungslos ablaufen und dass sie ihren Kunden einen kontinuierlichen Service bieten können.

Hochverfügbare Systeme sind auch in kritischen Infrastrukturen, wie beispielsweise in der Gesundheitsversorgung, in der Telekommunikation und im Finanzsektor, von entscheidender Bedeutung. In solchen Umgebungen kann selbst eine geringe Ausfallzeit erhebliche negative Auswirkungen haben, wodurch die Notwendigkeit der High-Availability noch verstärkt wird.

2.2 Überblick über den Ist-Zustand

Das Projekt, das dieses Sicherheitsupdate erhalten soll, ist das Federal Identity Management (FIM)-Portal, das sich auf das verteilte Identitätsmanagement konzentriert. Es bietet eine zentrale Plattform, über die sich Benutzer selbst onboarden und Vertrauensinstanzen, die neue Benutzer für das System freigeben und verwalten können. Webanwendungen können schnell in ein Dashboard eingebunden werden.

Die Webanwendungen, die Teil dieses Projekts sind, werden sowohl in-house, als auch von externen Anbietern entwickelt und im eigenen Rechenzentrum, oder außerhalb in einer externen Cloud gehostet.

Das FIM-Portal bietet eine breite Palette von Funktionen, darunter Benutzer-, Anmeldeinformations-, Richtlinien- und Zugriffsverwaltung. Es ermöglicht Entwicklern, Workflows zu erstellen, die Geschäftsprozesse abbilden, und diese Workflows an Anfragen anzuhängen. Benutzer können dann die Einhaltung von Geschäftsprozessen überwachen, indem sie beobachten, wie FIM Workflows ausgeführt werden.

2.2.1 SimpleSAMLphp

SimpleSAMLphp ist eine PHP-Bibliothek, die die Implementierung von SAML-basierten Single Sign-On-Systemen erleichtert. Es bietet Funktionen zur Authentifizierung, Autorisierung und Attribut-Abfrage und kann mit einer Vielzahl von Benutzerdatenquellen, einschließlich LDAP, integriert werden.

2.2.2 LinOTP

LinOTP ist ein Open-Source-Tool zur Generierung und Verifizierung von One-Time Passwords (OTPs). Es kann zur Implementierung von MFA verwendet werden, ist jedoch etwas umständlich und veraltet, da es hier bereits neue Produkte wie privacyIDEA gibt, welches ein Zweig von LinOTP ist und mit Hinsicht auf Keycloak eine Migrationsdokumentation hat.

2.2.3 LDAP

Lightweight Directory Access Protocol (LDAP) ist ein offenes, verteiltes Verzeichnisdiensteprotokoll, das zur Speicherung und zum Abrufen von Informationen über Benutzer, Gruppen und andere Ressourcen verwendet wird. SimpleSAMLphp unterstützt die Integration mit LDAP, einschließlich der Möglichkeit, LDAP-Benutzerattribute in das SAML-Benutzermodell zu mappen.

Kapitel 3

Methodik

In diesem Kapitel werden die Ansätze zur Untersuchung und Bewertung von OIDC-basierten SSO-Technologien ausführlich dargelegt. Nachdem die ausgewählten Vergleichskriterien analysiert und bewertet wurden, wird abschließend eine Nutzwertanalyse durchgeführt.

3.1 Auswahl der zu vergleichenden Technologien

Bei der Auswahl der zu vergleichenden Technologien beschränkt sich die vorliegende Seminararbeit auf Keycloak und Authentik. Beide sind OIDC-basierte SSO-Technologien, die jeweils unterschiedliche Vorteile und Eigenschaften aufweisen.

Die beiden Technologien wurden ausgewählt, um einen Vergleich zwischen einer etablierten und einer neueren Lösung zu schaffen und um zu zeigen, wie sie jeweils die Anforderungen an High-Availability, MFA und die einfache Integration von externen Dienstanbietern erfüllen.

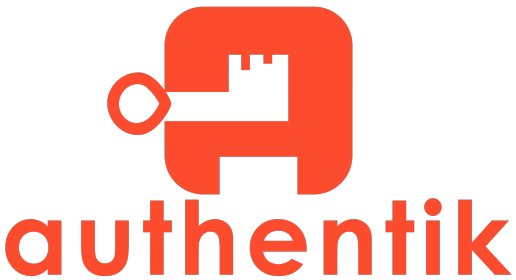

Abbildung 3.1: Authentik Logo

Abbildung 3.2: Keycloak Logo

3.1.1 Keycloak

Keycloak ist eine etablierte und weit verbreitete Open-Source-Lösung für Identity und Access Management (IAM). Es wird bereits im bestehenden Unternehmensumfeld eingesetzt, somit sind bereits Wissen und Expertise in dieser Technologie vorhanden. Keycloak bietet eine Vielzahl von Funktionen und unterstützt viele verschiedene Authentifizierungs- und Autorisierungsstandards. Es bietet eine hohe Benutzerfreundlichkeit und umfassende Verwaltungsoptionen.

Keycloak hat sich in der Praxis bewährt und als etabliertes Tool weist es viele Anwendungsfälle und eine ausführliche Dokumentation auf.

3.1.2 Authentik

Authentik ist eine neuere Open-Source-Lösung für IAM. Es wird als sehr vielseitig und benutzerfreundlich beschrieben und unterstützt verschiedene Authentifizierungsmethoden wie OIDC und SAML Protokolle.

Die Wahl von Authentik für diese Arbeit begründet sich in der leichten Implementierung und der breiten Palette von Funktionen. Darüber hinaus bietet Authentik ein gutes Preis-Leistungs-Verhältnis, welches zum Zeitpunkt der Veröffentlichung dieser Seminararbeit kostenlos ist, und daher eine wettbewerbsfähige Option gegenüber anderen Anbietern darstellt.

3.2 Vergleichskriterien

In diesem Abschnitt werden die Kriterien für den Vergleich der ausgewählten Technologien Keycloak und Authentik dargelegt. Diese Kriterien werden Aspekte wie Sicherheit, Benutzerfreundlichkeit, Integration mit externen Dienstleistern, Unterstützung von High-Availability und MFA berücksichtigen.

3.2.1 Merkmale

Keycloak ist bereits im Unternehmensumfeld etabliert und gilt als Standard für SSO-Tools, da es bereits länger auf dem Markt ist. Auch CANCOM setzt bereits auf diese Technologie und hat Keycloak für andere Projekte im Einsatz. Es bietet umfangreiche Funktionalitäten und hat bereits mehr Kapital als Authentik geschützt. Keycloak ist auch ein Projekt der Cloud Native Computing Foundation und wird von RedHat unterstützt.

Authentik ist wie Keycloak ein Open-Source-Projekt und hat eine aktive Community, die beispielsweise über Discord kommuniziert. Es hat auch eine umfangreiche Dokumentation und eine große Anzahl an Beiträgen. Dies deutet auf seine Qualität und Aktivität hin.

3.2.2 Authentifizierungsmethoden

Beide Technologien unterstützen sowohl OIDC als auch die SAML-basierte Authentifizierungsmethode, um Clients an den IdP anzubinden. [12] [10] Diese beiden sind die wesentlichen Technologien, die in dieser Seminararbeit von Relevanz sind, da sie im Fall von SAML bereits im Projekt implementiert sind und in der Übergangsphase weiter genutzt werden sollen, und OIDC, welches am Ende der Migration die gewünschte Technologie darstellt.

3.2.3 Unterstützung von MFA

Die Integration von MFA ist ein wichtiger Punkt zur Verbesserung der Sicherheit. Sowohl Keycloak als auch Authentik bieten umfangreiche Unterstützung für MFA, einschließlich verschiedener Authentifizierungsmethoden wie Time-based One-Time Password (TOTP), E-Mail und Web Authentication (WebAuthn).

Somit sind die bestehenden Authentifizierungsmechanismen weiter umsetzbar, zusätzlich besteht auch die Möglichkeit die neue WebAuthn-Methode zu implementieren und auch hier den Kundenwünschen gerecht zu werden.

Allerdings konnte keine Anbindung oder Migration gefunden werden, die es ermöglicht, einen bestehenden Datenbestand von LinOTP zu Authentik oder Keycloak zu migrieren. Daher müsste LinOTP zunächst in einem Parallelbetrieb weiter bestehen.

3.2.4 Sicherheit

Sowohl Keycloak als auch Authentik wurden bereits einem Penetrationstest unterzogen. Keycloak weist hier lediglich eine Schwachstelle von hoher und eine von niedriger Kritikalität auf. [4] Die fehlende Erfahrung von Authentik spiegelt sich auch im Penetrationstest wieder, hier wurden neben mehreren mittleren und hohen auch eine kritische Schwachstelle entdeckt. [7]

Es ist jedoch wichtig zu beachten, dass der Umfang dieser Tests unterschiedlich war und Sicherheitslücken in Softwareprodukten nicht ungewöhnlich sind. Entscheidend ist, wie schnell und effektiv die Entwickler auf solche Erkenntnisse reagieren und

die identifizierten Schwachstellen beheben. Hier können beide Technologien punkten.

3.2.5 Integration mit externen Dienstleistern

Sowohl Keycloak als auch Authentik, ermöglichen die Integration von externen Dienstleistern, im Umfang von SSO auch SPs genannt, was bedeutet, dass sie in der Lage sind, mit verschiedenen externen Anwendungen und Systemen zu kommunizieren.

Zudem bieten beide eine Vielzahl von Adaptern, die die Integration mit verschiedenen externen Dienstleistern erleichtern. Diese Adapter unterstützen gängige Protokolle wie SAML, OIDC und LDAP. Somit sind sowohl Keycloak als auch Authentik in der Lage mit verschiedenen externen Dienstleistern zu kommunizieren. Authentik ermöglicht die Einrichtung neuer Protokolle oder die Verfeinerung bestehender Protokolle innerhalb kurzer Zeit, was seine Flexibilität unterstreicht. Keycloak unterscheidet sich hier nur durch die Programmiersprache. Während Authentik auf Python setzt, werden Erweiterungen bei Keycloak in Java geschrieben.

3.2.6 Community und Support

Keycloak verfügt über eine umfangreiche und aktive Community. Sie bietet verschiedene Kanäle für Fragen und Hilfe, darunter Mailinglisten für Benutzer und Entwickler, die GitHub-Issues und ein Forum. [8] Darüber hinaus bietet Keycloak umfangreiche Dokumentationen und Anleitungen für verschiedene Aspekte der Verwendung und Konfiguration von Keycloak. [9]

Auch Authentik weißt eine umfangreiche Community auf. Benutzer können Feedback oder Fragen auf einem Authentik Discord-Server stellen, oder bei Schwierigkeiten und Verbesserungsvorschlägen auch in GitHub neue Issues eröffnen. Authentik bietet eine umfangreiche Dokumentation, die Benutzern die Möglichkeit bietet, die volle Funktionalität der Technologie zu nutzen. [14]

3.2.7 Benutzerfreundlichkeit

Einrichtung und Konfiguration

Die Einrichtung und Konfiguration beider Technologien, Keycloak und Authentik, wird durch ihre umfangreiche Dokumentation erleichtert. Dabei bieten beide Anleitungen für verschiedene Systeme an, wie zum Beispiel die Einrichtung in einer Docker- oder Kubernetes-Umgebung.

Keycloak bietet eine detaillierte Beschreibung zur Einrichtung und Konfiguration an, die auch komplexe Szenarien wie High-Availability abdeckt. Authentik hingegen

bietet eine vollständige Docker-Compose-Installation, die sowohl die Datenbanken Postgres und Redis als auch die Server-Worker-Konfiguration umfasst. Dies erleichtert die Einrichtung und den Einsatz von Authentik in einer produktiven Umgebung.

Die Communities stellen jedoch für Authentik einen Guide für eine High-Availability-Umgebung bereit und für Keycloak eine Docker-Compose-Konfiguration.

Benutzeroberfläche

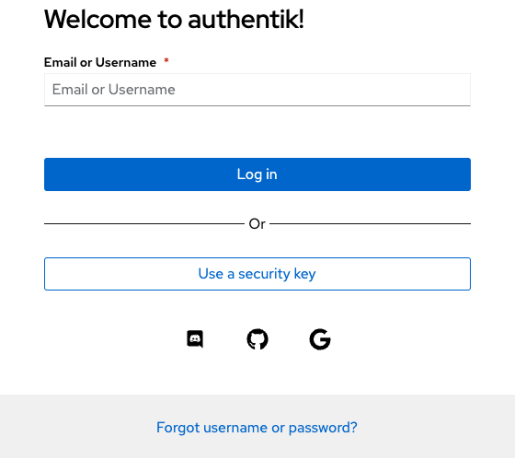

Abbildung 3.3: Authentik Login Karte

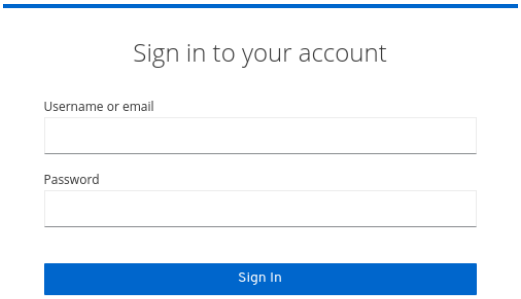

Abbildung 3.4: Keycloak Login Karte

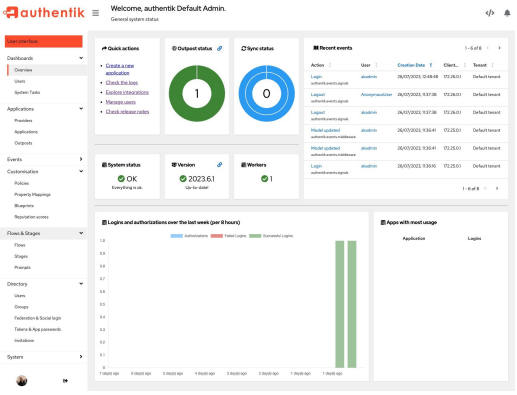

Abbildung 3.5: Authentik Administrator Seite

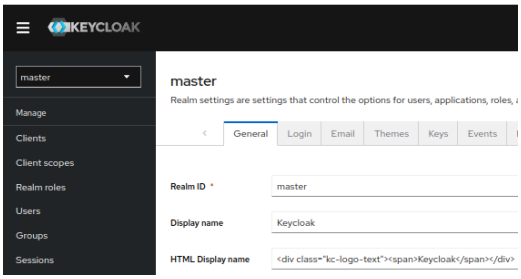

Abbildung 3.6: Keycloak Administrator Seite

Die Benutzeroberfläche spielt eine entscheidende Rolle in der Nutzererfahrung und in der Effizienz der täglichen Arbeit mit den Systemen. Keycloak bietet eine intuitive Administrationskonsole, die die Verwaltung von Benutzern, Rollen und Berechtigungen vereinfacht. Die Benutzeroberfläche von Authentik ist etwas moderner in ihrer Erscheinung und konzentriert sich stark auf die Benutzererfahrung.

3.2.8 Kosten

Keycloak und Authentik sind Open-Source-Technologien und in ihrem Standardumfang komplett kostenlos. Lediglich Authentik bietet eine Enterprise-Version an. Diese stellt einen erweiterten Support zur Verfügung und soll zukünftig weitere Features mit sich bringen. [11]

3.3 Auswertungsmethoden

In diesem Abschnitt werden die Auswertungsmethoden für die bewerteten Technologien diskutiert. Zunächst wird eine Nutzwertanalyse durchgeführt, um die Vor- und Nachteile jeder Technologie zu bewerten, und anschließend eine Nachbesprechung, um die Ergebnisse zu vergleichen und zu einer fundierten Entscheidung zu gelangen.

3.3.1 Nutzwertanalyse

„Die Nutzwertanalyse stellt eine leistungsfähige Planungsmethode dar. Sie dient der systematischen Entscheidungsvorbereitung durch Bewertung (Nutzenermittlung) und Auswahl (Rangfolge aufgrund des Nutzens) optimaler Alternativen (Bewertungsobjekte). Sie eignet sich besonders für Fälle, bei denen sich der Gesamtnutzen aus den unterschiedlichsten Teilnutzen zusammensetzt und der monetäre Gewinn als einziges Kriterium zur Entscheidungsfindung unzureichend ist. Die Nutzwertanalyse lässt die Erfassung sowohl objektiver als auch subjektiver Informationen zu.“ [1, Zusammenfassung]

Aufschlüsselung

Es ist wichtig zu beachten, dass die Punktzahl und der Gewichtungsfaktor für jedes Kriterium auf einer subjektiven Bewertung basiert und daher variieren kann, abhängig von den spezifischen Anforderungen und Prioritäten der Arbeit.

In der Nutzwertanalyse, siehe Seite 26, wird deutlich, dass Keycloak in Bezug auf High-Availability, MFA und Sicherheit eine höhere Punktzahl erhält, während Authentik in Bezug auf Integration und Benutzerfreundlichkeit mehr Punkte bekommt.

Die Gesamtpunktzahl und der Gewichtungsfaktor für Keycloak sind höher als für Authentik, was darauf hindeutet, dass Keycloak im Vergleich zu Authentik eine höhere Nutzwertzahl hat. Dies deutet darauf hin, dass Keycloak besser geeignet ist, um die Anforderungen an High-Availability, MFA und die einfache Integration von externen SPs zu erfüllen.

Auswertung

Obwohl Authentik in einigen Aspekten hinter Keycloak zurückbleibt, bietet es durch seine Benutzerfreundlichkeit einen Wettbewerbsvorteil. Keycloak hingegen erzielt mit 3.8 gewichteten Punkten einen höheren Nutzwert als Authentik (3.5) und wird daher nach der Nutzwertanalyse als bevorzugte Technologie empfohlen.

Es ist jedoch auch wichtig zu beachten, dass diese Analyse auf den Informationen basiert, die in dieser Arbeit zur Verfügung stehen. Weiterhin sind die Festlegung und die Gewichtung der Punkte immer subjektiver Natur und können unter Umständen auch anders ausfallen.

3.4 Nachbesprechung

In der Nachbesprechung wurden die bisherigen Ergebnisse der Forschung überprüft und validiert. Die Fachabteilungen, die bereits Erfahrungen mit Keycloak sammeln konnten und das FIM-Portal entwickeln, haben die Ergebnisse besprochen und Feedback gegeben.

Ein zentraler Punkt, der in der Nachbesprechung hervorgehoben wurde, ist die Notwendigkeit einer Migration von LinOTP zu Keycloak. Die Fachabteilungen haben darauf hingewiesen, dass LinOTP ein Zweig von privacyIDEA ist und dass es daher eine Möglichkeit geben könnte, von LinOTP zu Keycloak zu migrieren. Sie haben jedoch betont, dass diese Migration in einer weiteren Untersuchung weiter analysiert werden muss, um ihre Machbarkeit und Vorteile zu bestimmen.

Kapitel 4

Ergebnisse

In diesem Kapitel werden die Ergebnisse der Untersuchung und Bewertung von OIDC-basierten SSO-Technologien, insbesondere Keycloak und Authentik, präsentiert. Die Analyse basiert auf den in Kapitel 3 dargelegten Methoden und Kriterien.

4.1 Beantwortung der Forschungsfragen

In diesem Abschnitt werden die Forschungsfragen beantwortet, die im Kapitel 1.2 gestellt wurden.

4.1.1 Wie kann die SSO-Technologie mit OIDC zur Modernisierung eines Dienstes beitragen?

Die SSO-Technologie mit OIDC kann zur Modernisierung eines Dienstes beitragen, indem sie die Benutzererfahrung verbessert und die Sicherheit erhöht. OIDC ist ein Authentifizierungsprotokoll, das auf dem OAuth-Protokoll basiert und standardisierte Autorisierungsverfahren von OAuth verwendet, um Identitätsdienste bereitzustellen.

Mit OIDC können Entwickler ihre Benutzer über Websites und Apps authentifizieren, ohne eigenes Passwortmanagement betreiben und verwalten zu müssen. Dies bietet dem App-Entwickler eine sichere Möglichkeit, die Identität der Person zu überprüfen, die derzeit den Browser oder die native App verwendet, die mit der Anwendung verbunden ist.

Darüber hinaus ermöglicht OIDC die Implementierung von MFA, was die Sicherheit weiter erhöht. MFA erfordert, dass Benutzer mehr als ein Authentifizierungs-

merkmal bereitstellen, um auf Ressourcen zuzugreifen, was die Wahrscheinlichkeit, dass ein nicht autorisierter Benutzer Zugang erhält, erheblich verringert.

4.1.2 Wie kann die Implementierung von High-Availability und MFA in OIDC-basierten SSO-Systemen erreicht werden?

High-Availability kann durch die Verwendung von redundanten Systemen und Datenverteilung erreicht werden, um sicherzustellen, dass die Systeme auch dann verfügbar sind, wenn einzelne Komponenten ausfallen. Dies kann durch die Verwendung von Load-Balancern, Clustering und Datenreplikation erreicht werden.

MFA kann durch die Implementierung von mehrstufigen Authentifizierungsmechanismen erreicht werden. Dies kann durch die Verwendung von Passwörtern, biometrischen Daten, E-Mail-Bestätigungen oder Authentifizierungs-Apps erreicht werden. OIDC unterstützt MFA durch die Bereitstellung von Sicherheitstoken, die zur Authentifizierung und Autorisierung von Benutzern verwendet werden.

4.1.3 Wie können externe SP einfach in ein OIDC-basiertes SSO-System integriert werden?

Externe SP können einfach in ein OIDC-basiertes SSO-System integriert werden, indem sie als Clients in der OIDC-Authentifizierungs- und Autorisierungsaushandlung eingebunden werden. Dies erfordert, dass die SP in der Lage sind, OIDC-Anforderungen zu verstehen und zu verarbeiten, und dass sie mit dem OIDC-Provider kommunizieren können, um Authentifizierungs- und Autorisierungsanfragen zu senden und Antworten zu empfangen.

4.2 Ergebnisanalyse und Validierung

Die Punktzahl und der Gewichtungsfaktor für jedes Kriterium basieren auf einer subjektiven Bewertung und können daher variieren, abhängig von den spezifischen Anforderungen und Prioritäten der Arbeit. Die Gesamtpunktzahl und der Gewichtungsfaktor für Keycloak waren höher als für Authentik, was darauf hindeutet, dass Keycloak besser geeignet ist, um die Anforderungen an High-Availability, MFA und die einfache Integration von externen SP zu erfüllen.

Die Ergebnisse dieser Analyse wurden in einer Nachbesprechung mit allen Beteiligten validiert. Hierbei konnten die bisherigen Ergebnisse überprüft werden und

durch die Fachabteilungen, welche bereits Erfahrungen mit Keycloak sammeln konnte und aktiv am FIM-Portal entwickeln, validiert werden. Insgesamt ergab sich ein klares Bild für die Vorteile von Keycloak in Bezug auf die Anforderungen an High-Availability, und das bestehende Wissen, welches bereits zu Keycloak im Unternehmen existiert.

Die Kombination der Ergebnisse der Nutzwertanalyse und der Nachbesprechung hat dazu beigetragen, die Forschungsergebnisse zu validieren und Feedback von allen beteiligten Parteien zu erhalten. Die Diskussion in der Nachbesprechung führte dazu, die Forschungsergebnisse in einem Kontext zu verstehen und zu interpretieren.

4.3 Limitationen und kritische Reflexion

Während die Ergebnisse dieser Arbeit deutlich auf Keycloak als bevorzugte Technologie hinweisen, ist es wichtig, einige Einschränkungen und kritische Überlegungen zu beachten. Erstens basieren die Ergebnisse auf einer subjektiven Bewertung, die je nach spezifischen Anforderungen und Prioritäten variieren kann. Zweitens können die tatsächlichen Ergebnisse in der Praxis von den in dieser Arbeit präsentierten Ergebnissen abweichen, da die tatsächliche Sicherheit und Leistung auch stark von der korrekten Konfiguration und Verwendung der Technologien abhängt.

Trotz dieser Einschränkungen bieten die Ergebnisse dieser Arbeit wertvolle Einblicke in die Stärken und Schwächen von Keycloak und Authentik und können als Ausgangspunkt für weitere Untersuchungen und Entscheidungen dienen.

Kapitel 5

Ausblick

In diesem Kapitel werden die Auswirkungen und möglichen nächsten Schritte der Arbeit diskutiert.

5.1 Auswirkungen der Arbeit

Die Arbeit hat gezeigt, dass die Implementierung von OIDC-basierten SSO-Technologien wie Keycloak und Authentik zur Modernisierung eines Dienstes beitragen kann, indem sie die Benutzererfahrung verbessert und die Sicherheit erhöht. Es wurde deutlich, dass die Implementierung von High-Availability und MFA in OIDC-basierten SSO-Systemen erreicht werden kann und dass externe SP einfach in ein OIDC-basiertes SSO-System integriert werden können.

5.2 Nächste Schritte

Die nächsten Schritte könnten die Implementierung von Keycloak mit einem High-Availability-Setup über AWS und die Portierung der LinOTP-Daten umfassen. Darüber hinaus wäre es möglich die Integration von WebAuthn in Keycloak in Betracht zu ziehen. Diese Schritte könnten dazu beitragen, die Sicherheit und Benutzerfreundlichkeit des Dienstes weiter zu verbessern und die Integration mit externen SP zu erleichtern.

Literaturverzeichnis

[1] Gonde Dittmer. „Nutzwertanalyse“. In: *Managen mit Methode: Instrumente für individuelle Lösungen*. Hrsg. von Gonde Dittmer. Wiesbaden: Gabler Verlag, 1995, S. 43–56. ISBN: 978-3-663-05929-5. DOI: 10.1007/978-3-663-05929-5_5. URL: https://doi.org/10.1007/978-3-663-05929-5_5 (besucht am 09. 12. 2023).

[2] Bart De Win u. a. „On the importance of the separation-of-concerns principle in secure software engineering“. In: Workshop on the Application of Engineering Principles to System Security Design. Citeseer, 2002, S. 1–10.

[3] Aleksandr Ometov u. a. „Multi-factor authentication: A survey“. In: *Cryptography* 2.1 (2018). ISBN: 2410-387X Publisher: MDPI, S. 1.

[4] *Pentest-Report Keycloak 8.0 Audit & Pentest 11.2019*. 6. Feb. 2020. URL: https://cure53.de/pentest-report_keycloak.pdf (besucht am 17. 12. 2023).

[5] Lu Daniel. *What Is Single Sign-On (SSO)?* 19. Feb. 2021. URL: https://www.okta.com/blog/2021/02/single-sign-on-sso/ (besucht am 27. 11. 2023).

[6] Guido Schmitz. „Privacy-preserving Web single sign-on: Formal security analysis and design“. In: *it - Information Technology* 64.1 (1. Apr. 2022). Publisher: De Gruyter Oldenbourg, S. 43–48. ISSN: 2196-7032. DOI: 10.1515/itit-2022-0003. URL: https://www.degruyter.com/document/doi/10.1515/itit-2022-0003/html (besucht am 26. 11. 2023).

[7] *Pentest-Report authentik IdP Web, API & SSO 05.2023*. 23. Juni 2023. URL: https://cure53.de/pentest-report_authentik.pdf (besucht am 17. 12. 2023).

[8] *Community - Keycloak*. URL: https://www.keycloak.org/community (besucht am 17. 12. 2023).

[9] *Guides - Keycloak*. URL: https://www.keycloak.org/guides (besucht am 17. 12. 2023).

[10] *OAuth2 Provider — authentik*. URL: https://goauthentik.io/docs/providers/ (besucht am 04. 12. 2023).

[11] *Pricing — authentik*. URL: https://goauthentik.io/pricing/ (besucht am 17. 12. 2023).

[12] *Securing Applications and Services Guide*. URL: https://www.keycloak.org/docs/latest/securing_apps/ (besucht am 04. 12. 2023).

[13] *Was ist OpenID Connect und wofür wird es genutzt?* Auth0. URL: https://auth0.com/de/intro-to-iam/what-is-openid-connect-oidc#! (besucht am 17. 12. 2023).

[14] *Welcome to authentik — authentik*. URL: https://goauthentik.io/docs/ (besucht am 06. 12. 2023).

Kriterien	Gewichtung (%)	Keycloak		Authentik	
		Punkte	Gewichtet	Punkte	Gewichtet
High-Availability	10	4	0.4	3	0.3
Multi-Faktor Authentifizierung	20	4	0.8	3	0.6
Integration	20	4	0.8	5	1.0
Sicherheit	30	4	1.2	3	0.9
Benutzerfreundlichkeit	10	2	0.2	4	0.4
Community	10	4	0.4	3	0.3
Gesamt	100	22	3.8	21	3.5

Tabelle 1: Nutzwertanalyse von Keycloak und Authentik