



Abschlussprüfung Winter 2023

Fachinformatikerin für Systemintegration  
Dokumentation zur betrieblichen Projektarbeit

## **Implementierung von MFA**

**Implementierung von Multi-Faktor-Authentifizierung (MFA) zur  
Erhöhung der Sicherheit bei der Zugriffskontrolle von  
verschiedenen Services in einer Cloud-Infrastruktur**

Abgabetermin: Leipzig, den 27.11.2023

**Prüfungsbewerber:**

Melissa Futtig  
Stephaniplatz 3  
04317 Leipzig

**Deloitte.**

**Ausbildungsbetrieb:**

Deloitte Wirtschaftsprüfungsgesellschaft GmbH  
Dittrichring 22  
04109 Leipzig

# Winterprüfung 2023

## Ausbildungsberuf

Fachinformatiker/Fachinformatikerin (VO 2020) Fachrichtung: Systemintegration

## Prüfungsbezirk

Leipzig FISY 1 (AP T2V1)

Melissa Futtig

Identnummer: 886355

Prüflingsnummer: 52065

E-Mail: [mfuttig@deloitte.de](mailto:mfuttig@deloitte.de), Telefon: +49 1575283 33896

Ausbbildungsbetrieb: Deloitte GmbH Wirtschaftsprüfungsgesellschaft

Projektbetreuer: Edgar Kapler

E-Mail: [ekapler@deloitte.de](mailto:ekapler@deloitte.de), Telefon: +49 1515448 4702

## Thema der Projektarbeit

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

# 1 Thema der Projektarbeit

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## 2 Geplanter Bearbeitungszeitraum

Beginn: 30.10.2023

Ende: 10.11.2023

## 3 Ausgangssituation

In der Deloitte Wirtschaftsprüfungsgesellschaft GmbH wird die Sicherheit des Zugriffs auf verschiedene Dienste innerhalb einer Cloud-Infrastruktur verbessert, indem Multi-Faktor-Authentifizierung (MFA) eingeführt wird. Dies geschieht, um eine erhöhte Sicherheit für firmeninterne und kundenbezogene Daten zu gewährleisten.

### Ist-Analyse

Die Deloitte Wirtschaftsprüfungsgesellschaft GmbH verwendet die Cloud-Infrastruktur von OVHcloud, um einen Business Hosting Service bereitzustellen.

In dieser Konfiguration wird der Firewall eine öffentliche IP-Adresse zugewiesen. Das private Netzwerk enthält alle anderen Services und Instanzen und wird von der Firewall geschützt.

Eine Kontrollinstanz, namens „control\_node“, ermöglicht den Zugriff auf alle anderen Instanzen, die sich im privaten Netzwerk befinden.

Die Cloud-Infrastruktur ist in vier Hauptbereiche unterteilt, in denen verschiedene Services/Dienste bereitgestellt werden:

A) Compliance and Security Stack

- Bereich für Compliance und Sicherheit
- Hierzu gehören eine OPNsense Firewall, ein Nginx Proxy Manager, der als reverse Proxy für das HTTP-Protokoll dient und andere Ports als Stream weiterleitet, der Guacamole Server und das Open-Source-Sicherheitstesttool Infection Monkey

B) Monitoring

- Überwachungsbereich aller vorhandenen Dienste der Cloud-Infrastruktur
- Beinhaltet die Open-Source-Software Grafana, Uptime Kuma als Webserver und Healchecks

C) DevOps

- Bereich für die Entwicklung und Bereitstellung von Anwendungen
- Enthält die kollaborative Entwicklungsplattform Gitlab, Nexus zur Verwaltung von Repositories, Sonarqube für die statische Analyse und Bewertung von Quelltextqualität, sowie

## SFTPGO für die Authentifizierung mit öffentlichen Schlüsseln, SSH-Schlüsseln und Passwörtern

### D) E-Mail

- E-Mail-Bereich
- Umfasst den Mail-Server Mailcow und SOGO für die E-Mail-Kommunikation

Der Zugriff auf die o.g. Dienste erfolgt durch die Eingabe eines Nutzernamens und eines Passworts. Dies erzeugt eine potenzielle Sicherheitslücke und macht die Dienste unserer Cloud-Infrastruktur anfälliger für Phishing-Angriffe und unbefugten Zugriff.

### Soll-Konzept

Durch die Implementierung des MFA in der Cloud-Infrastruktur bei der Deloitte Wirtschaftsprüfungsgesellschaft GmbH soll durch das Hinzufügen einer weiteren Sicherheitsebene, Datenschutz und Integrität gewährleistet werden.

Die Deloitte Wirtschaftsprüfungsgesellschaft GmbH kann in alle Cloud-Services MFA integrieren, sodass durch dieses eine zusätzliche Sicherheitsebene aktiviert wird.

### Vorgang:

Zu Beginn erfolgt die Passworteingabe des Nutzers. Unter der Voraussetzung der Korrektheit, erhält dieser einen Sicherheitscode per SMS, E-Mail oder einer App, welcher eingegeben wird und zu einer erfolgreichen Anmeldung führt.

Mehrere fehlgeschlagene MFA-Versuche führen zu einer Sperrung des Kontos oder erfordern eine Rücksetzung durch den Administrator.

## 4 Projektziel

Das Hauptziel des Projekts besteht darin, die Sicherheit der Cloud-Infrastruktur der Deloitte Wirtschaftsprüfungsgesellschaft GmbH bei der Zugriffskontrolle auf die o.g. Services zu erhöhen, indem Multi-Faktor-Authentifizierung (MFA) eingeführt wird.

Dabei steht im Vordergrund das Ziel der Risikominimierung durch die Einführung einer zusätzlichen Authentifizierungsebene. Nur unter der Voraussetzung des zweiten Faktors kann eine erfolgreiche Anmeldung erfolgen.

Um die Arbeitsabläufe der Mitarbeiter nicht zu beeinträchtigen, wird darauf geachtet, die Benutzerfreundlichkeit aufrechtzuerhalten und die MFA-Lösung darauf zugeschnitten.

Die technische Umsetzung von Sitecars (Single Sign-On with Integrated Credential and Authentication System) für MFA ist eine effektive Methode, um die Sicherheit von Zugriffskontrollen auf verschiedene Services in unserer Cloud-Infrastruktur zu verbessern.

Diese Methode ermöglicht eine zentrale Verwaltung von Benutzeranmeldungen und -authentifizierung, wobei MFA eine zusätzliche Sicherheitsebene hinzufügt. Die Implementierung erfolgt in Docker-Container und ermöglicht eine einfache Bereitstellung und Portabilität zwischen verschiedenen Umgebungen.

Folgende Kriterien sollen erfüllt werden:

A) IT-Sicherheit

- Minimierung von Risiken, wie Passwort-Leaks und Phishing
- Anmeldung ist nur mit MFA möglich

B) Reibungsloser Benutzerzugriff

- Nutzerauthentifizierung, um Zugriff auf die o.g. Services zu erhalten
- Anmeldung/ Sperrung des Nutzers

C) Compliance

- Erfüllung von Sicherheits- und Datenschutzstandards

## 5 Zeitplanung

Planungsphase 5h

- Erstellen einer Ist-Analyse
- Erstellen einer Soll-Analyse
- Kostenplanung
- Projektumfeld
- Kosten- und Nutzanalyse
- Gantt-Diagramm
- Klärung der Projektziele

Implementierungsphase 14h

- Auswahl einer MFA-Lösung
- Installation und Konfiguration von Sitecars
- Konfiguration der MFA
- Integration mit Cloud-Diensten

Testphase 6h

- Überwachung der Laufzeit der Services
- Überprüfung/ Beseitigen von Fehlern
- Zugriffstests

Einführung und Übergabe 4h

- Ausführung und Ergebnisübergabe
- Schulung der zu Beteiligten für die Nutzung

Dokumentation 6h

- Erstellung einer Projektdokumentation der Ergebnisse
- Erstellung einer Entwicklerdokumentation

Gesamt: 35h

## 6 Anlagen

keine

## 7 Präsentationsmittel

- Laptop
- Beamer
- 5 Ausdrucke der Präsentation für den Notfall
- Ladekabel Laptop
- HDMI-Kabel
- USB-C Kabel
- PowerPoint

## 8 Hinweis!

Ich bestätige, dass der Projektantrag dem Ausbildungsbetrieb vorgelegt und vom Ausbildenden genehmigt wurde. Der Projektantrag enthält keine Betriebsgeheimnisse. Soweit diese für die Antragstellung notwendig sind, wurden nach Rücksprache mit dem Ausbildenden die entsprechenden Stellen unkenntlich gemacht.

Mit dem Absenden des Projektantrages bestätige ich weiterhin, dass der Antrag eigenständig von mir angefertigt wurde. Ferner sichere ich zu, dass im Projektantrag personenbezogene Daten (d. h. Daten über die eine Person identifizierbar oder bestimmbar ist) nur verwendet werden, wenn die betroffene Person hierin eingewilligt hat.

Bei meiner ersten Anmeldung im Online-Portal wurde ich darauf hingewiesen, dass meine Arbeit bei Täuschungshandlungen bzw. Ordnungsverstößen mit „null“ Punkten bewertet werden kann. Ich bin weiter darüber aufgeklärt worden, dass dies auch dann gilt, wenn festgestellt wird, dass meine Arbeit im Ganzen oder zu Teilen mit der eines anderen Prüfungsteilnehmers übereinstimmt. Es ist mir bewusst, dass Kontrollen durchgeführt werden.

## 9 Grund für „mit Auflage genehmigt“

Guten Tag Melissa Futtig,  
bitte achten Sie darauf, dass Ihre "Projektdokumentation der Ergebnisse" auch die Projektarbeit für den Prüfungsausschuss wiederspiegelt. In der Fachrichtung Systemintegration wird keine Entwicklerdokumentation erwartet, aber eine Kunden- und/oder Benutzerdokumentation (siehe



Handreichung der IHK <https://www.leipzig.ihk.de/mb-04-112/>). Unglücklich ist die "Klärung der Projektziele" am Ende der Planung. Berücksichtigen Sie gegebenenfalls, dass Ihnen nach neuer Verordnung 40 Stunden für die Projektarbeit zur Verfügung stehen.

mit Auflage genehmigt

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## Inhaltsverzeichnis

---

<b>1</b>	<b>Problemstellung</b>	<b>1</b>
<b>2</b>	<b>Ist/Soll-Analyse</b>	<b>1</b>
2.1	Projektumfeld . . . . .	1
2.2	Projektaufgabe . . . . .	2
2.3	Projektziel . . . . .	2
2.4	Projektschnittstellen . . . . .	2
2.4.1	Technisch . . . . .	2
2.4.2	Organisatorisch . . . . .	4
2.4.3	Personell . . . . .	4
2.5	Anforderungsanalyse . . . . .	4
2.5.1	Funktionale Anforderungen . . . . .	4
2.5.2	Nicht-Funktionale Anforderungen . . . . .	5
<b>3</b>	<b>Projektplanung</b>	<b>5</b>
3.1	Projektphasen . . . . .	5
3.2	Authentifizierungs-Tool . . . . .	6
3.3	Ressourcenplanung . . . . .	7
3.3.1	Sachmittelplanung . . . . .	7
3.3.2	Personalplanung . . . . .	7
3.4	Kostenplanung . . . . .	8
3.5	Wirtschaftlichkeitsanalyse . . . . .	8
3.5.1	Ablaufplanung und Meilensteine . . . . .	9
3.6	Amortisationsdauer . . . . .	9
3.7	Nicht-monetärer Nutzen . . . . .	10
3.8	Abweichungen vom Projektantrag . . . . .	10
3.9	Entwicklungsprozess . . . . .	11
<b>4</b>	<b>Projektdurchführung</b>	<b>11</b>
4.1	Vorbereitung der Entwicklungsumgebung . . . . .	11
4.2	Auswahl einer MFA-Lösung . . . . .	12
4.3	Erstellung der docker-compose.yml und .env . . . . .	12
4.4	Konfiguration des NGinx Reverse Proxy Managers . . . . .	13
4.5	Konfiguration von Authentik . . . . .	14
4.6	Integration mit Cloud-Diensten . . . . .	14
4.7	Einrichtung des zweiten Faktors . . . . .	14
4.8	Maßnahmen zur Qualitätssicherung . . . . .	15
4.8.1	Produktorientierte Maßnahmen . . . . .	15
4.8.2	Prozessorientierte Maßnahmen . . . . .	15
<b>5</b>	<b>Test- und Abnahme</b>	<b>15</b>

# **IMPLEMENTIERUNG VON MFA**

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## *Inhaltsverzeichnis*

---

5.1	Überwachung der Laufzeit der Dienste . . . . .	15
5.2	Überprüfung/ Beseitigung von Fehlern . . . . .	16
5.3	Zugriffstests . . . . .	16
5.4	Abnahme . . . . .	16
<b>6</b>	<b>Dokumentation</b>	<b>16</b>
6.1	Benutzerdokumentation . . . . .	16
<b>7</b>	<b>Fazit</b>	<b>17</b>
7.1	Soll-/Ist-Vergleich . . . . .	17
7.2	Gewonnene Erkenntnisse . . . . .	17
7.3	Ausblick . . . . .	17
<b>A</b>	<b>Anhang</b>	<b>18</b>
	Abkürzungsverzeichnis . . . . .	18
	Begriffserklärung . . . . .	19
A.1	Gantt-Diagramm und Meilensteine . . . . .	20
A.2	Detaillierte Zeitplanung . . . . .	21
A.3	Use Case-Diagramm . . . . .	22
A.4	Sequenzdiagramm CLI Zugriff auf die Instanzen . . . . .	23
A.5	Cloud-Infrastruktur . . . . .	24
A.6	docker-compose.yml . . . . .	25
A.7	.env . . . . .	26
A.8	Docker-Befehle . . . . .	27
A.9	Proxy Host Konfiguration . . . . .	28
A.10	Authentik-Konfiguration . . . . .	29
A.11	NGinx Konfiguration . . . . .	32
A.12	TOTP-Einrichtung . . . . .	34
A.13	Benutzerdokumentation . . . . .	35
A.14	Testprotokoll . . . . .	36
A.15	Übernahmeprotokoll . . . . .	37
	<b>Abbildungsverzeichnis</b>	<b>38</b>
	<b>Tabellenverzeichnis</b>	<b>39</b>
	<b>Literaturverzeichnis</b>	<b>40</b>
	<b>Eidesstattliche Erklärung</b>	<b>41</b>
	<b>Nachweis zur Durchführung der betrieblichen Projektarbeit</b>	<b>42</b>

## IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

### 1 Problemstellung

---

Die zunehmende Bedeutung von Cloud-Infrastrukturen für Unternehmen geht einher mit der Herausforderung, eine robuste Sicherheitsarchitektur zu etablieren. Die Deloitte Wirtschaftsprüfungsgesellschaft GmbH, als Anbieter von umfassenden Unternehmensdienstleistungen, steht vor der Notwendigkeit, die Sicherheit und Vertraulichkeit ihrer Cloud-basierten Dienste zu erhöhen. Aktuelle Sicherheitsmechanismen reichen nicht aus, um den ständig wachsenden Bedrohungen und Angriffen auf Unternehmensdaten wirksam zu begegnen. Insbesondere der Zugang zu sensiblen Informationen über die Cloud-Infrastruktur birgt ein hohes Risiko, das durch die herkömmliche Authentifizierung mittels Benutzername und Passwort allein nicht ausreichend adressiert wird. Das Fehlen einer zusätzlichen Sicherheitsebene in Form einer Multi-Faktor-Authentifizierung (MFA) lässt potenzielle Schwachstellen offen, die es Angreifern ermöglichen könnten, über gestohlene Zugangsdaten unbefugten Zugriff zu erlangen. Diese Lücke in der Sicherheitsstrategie unterstreicht die Notwendigkeit eines Projektes, das die Einführung einer MFA-Lösung für die Cloud-Infrastruktur der Deloitte GmbH fokussiert. Durch die Implementierung einer MFA wird nicht nur die Sicherheit des Zugriffs auf die Dienste erhöht, sondern auch das Vertrauen der Kunden gestärkt und das Risiko von Datenlecks und Phishing-Angriffen minimiert.

## 2 Ist/Soll-Analyse

### 2.1 Projektumfeld

Die [DELOITTE \[2023\]](#) Wirtschaftsprüfungsgesellschaft GmbH ist ein internationales Unternehmen für Wirtschaftsprüfung, Steuer-, Unternehmens-, Risiko- und Finanzberatung. Sie hat Niederlassungen in vielen Ländern, darunter auch Deutschland. Mit Vertrettern in über 150 Ländern weltweit und 415.000 Mitarbeitern, bietet das Unternehmen eine breite Palette von Dienstleistungen für Unternehmen und Organisationen in verschiedenen Branchen. Im B and TCL, auch Business & Technology Center Leipzig genannt, erbringt die Deloitte GmbH mit ihren 100 Mitarbeitern eine Vielfalt an Business Services, mit und ohne IT-Bezug und treibt Transformationsprojekte rund um die Themen Cyber Security, Digitalisierung, Prozessoptimierung oder Automatisierung voran.

Das Projekt mit dem Fokus auf Multi-Faktor-Authentifizierung bei verschiedenen Services in einer Cloud-Infrastruktur ist ein Tochterprojekt eines Größeren. Dabei ist gemeint, dass dieses "Tochterprojekt" nicht alleine existiert, sondern als Teil des größeren Projektes agiert. Die Deloitte Wirtschaftsprüfungsgesellschaft GmbH verwendet die Cloud-Infrastruktur von [OVH CLOUD \[2023\]](#), um einen Business Hosting Service bereitzustellen. Die Zielgruppe stellt das Projektteam dar, welche in dem größeren Projekt mit entwickeln.

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## 2 Ist/Soll-Analyse

---

### 2.2 Projektaufgabe

Der Zweck des Projektes ist es, den Entwicklern der Cloud-Infrastruktur mit den darauf gehosteten Services bzw. Diensten, eine Authentifizierungsmöglichkeit zu bieten, die die Sicherheit des Einloggens erhöht. Die Aufgabe besteht darin, die Entwicklungsumgebung vorzubereiten und einzurichten, indem Docker als eine Containerisierungstechnologie, installiert sein muss, um die Docker-Dateien für die Containerisierung erst zu erstellen und schlussendlich auszuführen. Im Anschluss wird die MFA-Lösung eingerichtet. Dazu gehört das Hinzufügen der Dienste und die Aktivierung von MFA. Schlussendlich wird der Fokus nach der Fertigstellung der Entwicklungsumgebung auf das Testen der MFA-Lösung gesetzt und das vollständige Ergebnis in die Produktivumgebung umgesetzt.

### 2.3 Projektziel

Ziel ist es, die Sicherheit des Zugriffs auf verschiedene Dienste innerhalb dieser Cloud-Infrastruktur zu verbessern, indem Multi-Faktor-Authentifizierung (MFA) eingeführt wird. Dadurch soll eine erhöhte Sicherheit für firmeninterne und kundenbezogene Daten gewährleistet werden, indem nur eine Anmeldung mit MFA möglich ist und resultierend daraus Risiken, wie Passwork-Leaks und Phishing vermieden werden können. Um das Ziel zu erreichen, soll eine MFA-Lösung implementiert werden, welche sich vor die verschiedenen Dienste in der Cloud-Infrastruktur schaltet und den Zugriff der Benutzer verwalten und sichern soll.

### 2.4 Projektschnittstellen

#### 2.4.1 Technisch

Die besagte Cloud-Infrastruktur ist in vier Hauptbereiche unterteilt, wobei in jedem Bereich verschiedene Dienste, inklusive die MFA-Lösung Authentik, welche mit allen Diensten interagiert, über Docker-Container bereitgestellt werden.

##### *Compliance and Security Stack*

Dieser Bereich umfasst den Einsatz, wie die OPNsense Firewall, den NGinx Proxy Manager, dem Authentik- und Guacamole Server und Infection Monkey zur Sicherheitsüberprüfung. Zusammenfassend ist zu sagen, dass der NGinx Proxy Manager als Reverse Proxy fungiert und den HTTP-Verkehr umleitet und andere Ports für Streaming-Anforderungen bedient. Mittels von Apache Guacamole erfolgt die Sicherstellung des Fernzugriffs auf die internen Dienste, die regulär nicht über eine Web-Schnittstelle erreichbar sind. Das Open-Source-Sicherheitstesttool Infection Monkey überprüft die Sicherheit der Infrastruktur. Mit dem Identitätsanbieter [AUTHENTIK \[2023\]](#), werden verschiedene Identitäts- und Authentifizierungsmethoden in Anwendungen und Diensten ermöglicht, zu integrieren. Dadurch wird eine wichtige Schnittstelle für die Benutzerauthentifizierung und -autorisierung bereitgestellt und kann von verschiedenen Anwendungen über Docker-Container Authentifizierungsmechanismen einrichten.

## IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

### 2 Ist/Soll-Analyse

---

#### *Monitoring*

Im Überwachungsbereich agiert die Open-Source-Software Grafana für die Visualisierung und Überwachung von Leistungsdaten, sowie Uptime Kuma als Webserver für Statusseiten und Healthchecks, um die Verfügbarkeit der Dienste zu kontrollieren.

#### *DevOps*

Der Fokus liegt bei den Anwendungen in der Entwicklung und Bereitstellung und enthält die Kollaborationsplattform GitLab, um beispielsweise Projekte zu verwalten. Nexus kommt als Verwaltungstool der Repositories für die Anwendungsabhängigkeiten zum Einsatz. Sonarqube ermöglicht die statische Analyse und Bewertung der Quelltextqualität. Zusätzlich wird SFTPGO verwendet, um sichere Authentifizierungsmethoden, wie zum Beispiel SSH-Schlüssel und Passwörter zu verwalten.

#### *E-Mail-Kommunikation*

In diesem Bereich agiert der Mail-Server Mailcow, um E-Mails zu senden und empfangen, SOGO als Groupware-Lösung, was eine effiziente E-Mail-Kommunikation und Zusammenarbeit innerhalb und außerhalb des Unternehmens ermöglicht.

Für dieses Projekt werden insgesamt drei Instanzen des Anbieters OVH-Cloud für Cloud-Computing-Dienste genutzt. Alle drei Instanzen sind Linux-Systeme mit Ubuntu und variieren in ihren Ressourcen wie RAM und CPU. Auf diesen Instanzen werden die im Kapitel genannten Dienste durch Containerisierung betrieben. Jeder Instanz wird zur besseren Zuordnung eine spezifische Bezeichnung zugeordnet. Die erste Instanz, genannt **"control\_node"**, fungiert als Anlaufstelle, an der sich Benutzer zu Beginn verbinden müssen. Diese Instanz dient als Kontrollpunkt, über den der Zugang zu den anderen Instanzen erfolgt. Sie fungiert gewissermaßen als Gateway zu entweder der Instanz **"rev\_prox\_dev"** oder der **"tal\_cloud\_infra"**. Der Zugriff auf diese Instanzen geschieht mittels eines SSH-Schlüssels von einem lokalen Notebook aus über die Kommandozeile. Alle Dienste, auch Authentik, bis auf den NGinx Reverse Proxy Manager, sind auf der **"tal\_cloud\_infra"** lokalisiert. Letzterer läuft auf der **"rev\_prox\_dev"**-Instanz. Die Bezeichnung **"tal\_cloud\_infra"** bezieht sich auf den Standort Deloitte in Leipzig, bekannt als **B und TAL!**. **"rev\_prox\_dev"** erhält seinen Namen aufgrund des dort laufenden NGinx Reverse Proxy Managers. Ein Diagramm, das den Zugriff eines Benutzers auf eine Instanz über die CLI veranschaulicht, befindet sich im Anhang Sequenzdiagramm CLI Zugriff auf die Instanzen.

Ein Use Case-Diagramm zur Veranschaulichung des Prozesses der Cloud-Infrastruktur findet sich im Anhang A.3 Use Case-Diagramm. In diesem interagiert der Akteur aus der Sicht eines Projektentwicklers mit dem System, in welchem verschiedene Anwendungsfälle existieren. Der Akteur meldet sich über den Authentik Server bei der Firewall und dem Nginx Proxy Manager an. Nach der erfolgreichen Anmeldung mit der MFA hat dieser die Möglichkeit auf die dann zur Verfügung stehenden Dienste vom Nginx Reverse Proxy Manager aus zuzugreifen.

Hat sich der Akteur mit dem Authentik Server verbunden, der aus dem dem eigentlichen Server (Authentik Core Server) und dem integrierten Außenposten (Embedded outpost) besteht, werden einkommende Anfragen an den Server-Containern und den Authentik Core Server und dem Embedded oupost geroutet. Der Authentik Core Server verarbeitet den Großteil der Logik von Authentik, wie z. B. API- und/ oder SSO-Anfragen, während der Embedded outpost die Verwendung von Proxy-Anbietern ermöglicht, ohne dass eine separate Außenstelle eingerichtet

## IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

### 2 Ist/Soll-Analyse

---

werden muss. Der Hintergrundarbeiter (Background Worker) führt Hintergrundaufgaben aus, wie das Senden von E-Mails, oder Benachrichtigen von Ereignissen und alles, was im Frontend sichtbar ist. Authentik nutzt PostgreSQL, um alle seiner Konfigurationen und Daten zu speichern. Redis wird als Message-Queue und Cache verwendet.

#### **2.4.2 Organisatorisch**

Nach der Integration der MFA-Lösung in die Cloud-Umgebung werden zunächst Tests und Überprüfungen in den konfigurierten Docker-Containern mithilfe der *docker-compose.yml*-Datei durchgeführt. Dies gewährleistet eine ordnungsgemäße Funktionsweise und die Erfüllung der Sicherheitsstandards. Im Anschluss erfolgen Schulungen der Benutzer, in dem Fall für das Entwicklerteam, zur genauen Verwendung von Authentik mit MFA. Nach den Tests und der Schulungen des Entwicklerteams wird die MFA-Implementierung in der Cloud-Umgebung bereitgestellt.

#### **2.4.3 Personell**

Das Projektteam besteht aus folgenden Personen:

- Projektleiter/ Manager/ Projektentwickler: Herr Edgar Johann Kapler
- Tester/ dualer Student: Herr Birk Spinn
- Projektentwicklerin/ Auszubildende: Frau Melissa Futtig

Der Projektleiter ist der Verantwortliche für die Projektleitung und -finanzierung des Projektes. Er genehmigt dieses und stellt die notwendigen Ressourcen zur Entwicklung zur Verfügung. Die Projektentwickler sind die allgemeinen Benutzer bzw. das Entwicklerteam. Sie sind für die Umsetzung und den reibungslosen Betrieb der Cloud-Infrastruktur verantwortlich und benötigen sichere Zugriffsmöglichkeiten zu den bereitgestellten Anwendungen.

## **2.5 Anforderungsanalyse**

### **2.5.1 Funktionale Anforderungen**

Die MFA-Lösung muss folgende funktionale Anforderungen erfüllen:

- Benutzerfreundliche Registrierung und Login
- Klare Anleitung für die Einmalpasswort-Eingabe
- Übersichtliche Verwaltung von Nutzern
- Einloggen als Admin und Benutzer
- Dienste nach Benutzerdateneingabe aktivieren

## IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

### 3 Projektplanung

---

- Schutz vor Drittzugriff, sichere Lösung
- Nutzung mit Authentikator-Software

#### 2.5.2 Nicht-Funktionale Anforderungen

Die MFA-Lösung muss folgende nicht-funktionale Anforderungen erfüllen:

- Skalierbarkeit der Dienste
- Weiterleitung zu den Diensten in unter 2 Sekunden
- Übersichtliches Willkommensdisplay
- Verfügbarkeit einer englischen Oberfläche

## 3 Projektplanung

### 3.1 Projektphasen

Die im Projektantrag festgelegten Projektphasen lassen sich chronologisch in die 8-stündige Planungsphase, die 16-stündige Implementierungsphase, die 4-stündige Testphase, die 4-stündige Phase der Einführung und Übergabe und die 8-stündige Dokumentation einteilen. Dabei änderte sich die Zeit in der Implementierungsphase von 14 auf 16 Stunden, die Zeit in der Dokumentation von 6 auf 8 Stunden.

Das Projekt findet in zwei Wochen, vom 30.10.2023 bis zum 10.11.2023 statt.

Tabelle 1 Zeitplanung zeigt ein Beispiel für eine grobe Zeitplanung. Eine detailliertere Zeitplanung befindet sich im Anhang Zeitplanung.

Projektphase	Geplante Zeit
Planungsphase	8 h
Implementierungsphase	16 h
Testphase	4 h
Einführung und Übergabe	4 h
Dokumentation	8 h
<b>Gesamt</b>	<b>40 h</b>

Tabelle 1: Zeitplanung

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## 3 Projektplanung

---

### 3.2 Authentifizierungs-Tool

Anhand der Entscheidungsmatrix in Tabelle 2 wurde Authentik ausgewählt.

Die Gewichtung bildet sich durch den Gesamtwert von 100 Wertungspunkten mit einem Maximalwert von 25 und Mindestwert von 10 Punkten. Grund dafür sind die unterschiedlichen Eigenschaften, welche in der Entwicklung und bei der Auswahl der Authentifizierungsmethode jeweils verschiedene Rollen spielen und folglich daraus evaluiert werden. Nach der Zuordnung und Addierung der Punkte bei den vier Authentifizierungs-Tools, wird die Gesamtheit aller Punkte eines Produktes durch den Wert 100 dividiert und das Endergebnis ausgerechnet. Dabei hat die Einhaltung der Sicherheit Priorität und erhält den Maximalwert von 25 Punkten, aufgrund dessen, dass Dritten der Zugriff auf die jeweiligen Dienste mit kunden- und firmeninternen Daten der Cloud-Infrastruktur verweigert werden sollte. Die MFA wird mit 20 Punkten bewertet, weil dass das Ziel des Projektes ist. Die Benutzerfreundlichkeit, das Implementieren mit Open-Source und die Skalierbarkeit erhalten 15 Punkte, weil jeder User schnell und einfach auf den jeweiligen Dienst zugreifen muss. Für dieses Projekt ist es des Weiteren wichtig, ein Tool zu implementieren, was den zeitlichen Rahmen nicht überschreitet und die Gesamtheit der Einführung zu komplex gestaltet. Die Skalierbarkeit hat für das Projekt eine durchschnittliche Relevanz, da die Möglichkeit bestehen soll, Dienste hinzuzufügen oder rauszunehmen. Am wenigsten bedeutend sind die Erfahrungswerte, welche gleichermaßen nicht zu unterschätzen sind, weil eine Community über das Produkt bei der Entwicklung unterstützend wirkend kann.

Dabei erhält Authentik den größten Nutzwert mit 17,05 Punkten und schneidet vor Authelia, Microsoft Azure AD und Sitecar am besten ab. Aus diesem Grund wird sich für Authentik anstatt für Sitecar entschieden, da besonders die Implementierungsdauer und -komplexität bei Sitecar den Rahmen des Projektes sprengen würde.

Eigenschaft	Wertung	Authentik	Authelia	Sitecar	Mic. AD
Benutzerfreundlichkeit	15	15	15	12	14
Sicherheit (OIDC, LDAP)	25	25	17	18	20
Open-Source	15	15	15	9	7
MFA	20	19	20	14	19
Skalierbarkeit	15	12	14	12	15
Erfahrungswerte	10	7	9	3	10
<b>Gesamt:</b>	<b>100</b>	<b>93</b>	<b>90</b>	<b>68</b>	<b>85</b>
<b>Nutzwert:</b>		<b>17,05</b>	<b>15,75</b>	<b>12,55</b>	<b>15,20</b>

Tabelle 2: Entscheidungsmatrix

Dabei steht *Mic. Az.* für Microsoft Azure.

Die zu resultierende Zielplattform definiert sich über die Benutzerfreundlichkeit, die Sicherheit und dem Fokus auf der Interaktion mit OIDC und LDAP, welche zukünftig für das Projekt vorgesehen sind, sowie der Implementierung vom Open-Source, dem Arbeiten mit MFA, der Skalierbarkeit und den Erfahrungswerten von anderen Entwicklern mit dem entsprechenden Produkt. Das Resultat wird im Kapitel 3.2: Authentifizierungs-Tool der dargestellten Entscheidungsmatrix sichtbar.

## IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

### 3 Projektplanung

---

#### 3.3 Ressourcenplanung

##### 3.3.1 Sachmittelplanung

Um die Umsetzung des Projektes zu ermöglichen, wurden folgende Hard- und Software verwendet:

- Notebook - Lenovo ThinkPad T15 Gen 1 (für die Entwicklung)
- Betriebssystem - Microsoft Windows 10 Enterprise auf dem Lenovo-Notebook
- iPhone 12 - iOS 17.0.3 (zum Testen des Einmalpassworts)
- Microsoft Authenticator (auf dem iPhone 12 vorinstalliert)
- IDE - Visual Studio Code 1.83.1 (Benutzereinstellung)
- Docker-Containerisierung auf der OVH-Cloud-Infrastruktur in einer Linux-Umgebung mit Ubuntu 22.04
- OVH-Cloud-Instanz - firewall\_instance\_dev
- OVH-Cloud-Instanz - tal\_cloud\_infra
- OVH-Cloud-Instanz - rev\_prox-dev
- Google Chrome - Browser

Die von OVH-Cloud gestellten Instanzen sind Cloud-Instanzen mit Linux-Umgebungen, auf denen die Containerisierungen laufen. Dabei wurde im Kapitel 2.4 Projektschnittstellen detaillierter auf die Namen der jeweiligen Instanzen eingegangen.

##### 3.3.2 Personalplanung

Tabelle 3 zeigt die Personalplanung des Projektes.

Name	Rolle/ Berufsbezeichnung	Zeitaufwand
Edgar Johann Kapler	Manager	2 h
Birk Spinn	dualer Student	3 h
Melissa Futtig	Auszubildende	40 h

Tabelle 3: Personalplanung

In diesem Projekt arbeitet die Autorin Melissa Futtig 40 Stunden am Projekt, während der Projektmanager Edgar Johann Kapler 2 Stunden für das Testen der Anwendung und dem Übergabeprozess aufwendet, da ihm das Ergebnis des Projektes schlussendlich übergeben wird. Der duale Student Birk Spinn unterstützt bei der Implementierung und dem Testen der Anwendung und benötigt für diese Aufgaben insgesamt 3 Stunden.

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## 3 Projektplanung

---

### 3.4 Kostenplanung

Die Kosten für die Durchführung des Projekts setzen sich aus den Personal- und Ressourcenkosten zusammen. Das Brutto-Einkommen eines Auszubildenden im 3. Lehrjahr im Fachbereich Fachinformatik bei der Deloitte Wirtschaftsprüfungsgesellschaft GmbH beträgt 1400,00 € pro Monat. Zu den 1400,00 € kommen 1090,00 € Versicherungskosten dazu, die die Deloitte bezahlt. Die reguläre Arbeitszeit in einer normalen Arbeitswoche von Montag bis Freitag beträgt 40 Stunden, 8 Stunden am Tag und 220 Arbeitstage im Jahr. Die 220 Tage entstehen, da von den 365 Tagen eines Kalenderjahres 104 Wochenendtage, 11 Feiertage und 30 Urlaubstage abgezogen. Für die weiteren Mitarbeiter werden pauschale Beträge zur Berechnung des Stundensatzes genutzt. Duale Studenten werden pauschal mit 15,00 €, während die Manager mit 75,00 € pro Stunde berechnet werden. Bei jeweils beiden addiert sich die Summe der Ressourcenkosten auf. Anhand der oben genannten Formel ergibt sich ein Stundenlohn von 9,55 €. Dieser wird aus dem Brutto-Einkommen des Auszubildenden berechnet.

Die Durchführungszeit des Projekts beträgt 40 Stunden. Die Anforderungen durch die Ressourcen, wie der Stromverbrauch, die zu verwendende Hardware und die Räumlichkeiten, sowie das Büromaterial, wie z. B. der zu nutzende Monitor, die Peripheriegeräte (Maus, Tastatur, etc.) und das Mobiliar zusammen. Der Mittelwert wird pauschal mit 15,00 € kalkuliert.

$$8 \text{ h/Tag} \cdot 220 \text{ Tage/Jahr} = 1760 \text{ h/Jahr} \quad (1)$$

$$2490 \text{ €/Monat} \cdot 12 \text{ Monate/Jahr} = 29880 \text{ €/Jahr} \quad (2)$$

$$\frac{29880 \text{ €/Jahr}}{1760 \text{ h/Jahr}} \approx 16,98 \text{ €/h} \quad (3)$$

Die Gesamtkosten, dargestellt in der Tabelle 4 betragen 1.561,88 €.

Vorgang	Zeit	Kosten pro Stunde	Kosten
Arbeitskosten	40 h	$16,98 \text{ €} + 15,00 \text{ €} = 31,98 \text{ €}$	1.279,20 €
Unterstützungskosten (Manager)	2 h	$75,00 \text{ €} + 15,00 \text{ €} = 90,00 \text{ €}$	180,00 €
Unterstützungskosten (dualer Student)	3 h	$15,00 \text{ €} + 15,00 \text{ €} = 30,00 \text{ €}$	90,00 €
OVH-Cloud-Kosten	40 h	$0,317 \text{ €} + 0,00 \text{ €} = 0,317 \text{ €}$	12,68 €
			<b>1.561,88 €</b>

Tabelle 4: Kostenaufstellung

### 3.5 Wirtschaftlichkeitsanalyse

Durch die schon vorhandene Cloud-Infrastruktur des größeren Projektes entstehen keine weiteren Kosten. Bedingt dessen, dass die OVH-Cloud-Infrastruktur zu einem Fix-Preis pro Instanz gemietet wird und keine weiteren Instanzen für die Implementierung des Tochter-Projektes erforderlich sind, bleiben die Kosten unverändert. An Ressourcen wird zwar mehr CPU und Rechenleistung

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## 3 Projektplanung

---

verwendet, was allerdings nicht nach dem [PAY-As-You-Go \[2023\]](#)-Prinzip berechnet wird, sondern bei OVH-Cloud pauschal nach Instanzpreis, sodass für das "Tochter-Projekt" keine weitere Kosten entstehen. In dem Pay-As-You-Go-Prinzip werden nur die Ressourcen bezahlt, die auch tatsächlich genutzt werden. Die wirklich zu entstehenden Kosten sind ausschließlich Personal- und Materialkosten, wobei letztere aus der Nutzung des Büromobiliars und der Strom- und Heizkosten zusammengefasst wird.

Durch die Einführung der MFA-Lösung in der Cloud-Infrastruktur werden besonders die Schutzziele der Einhaltung der Integrität und Vertraulichkeit der Daten auf den jeweiligen Diensten eingehalten. So wird die Sicherheit erheblich verbessert und trägt dazu bei, unbefugten Zugriff, Datenverluste und Betrug zu verhindern. Dieser Schutz vor Sicherheitsverletzungen kann erhebliche finanzielle Auswirkungen haben, da die Wiederherstellungskosten vermieden werden können. Zusätzlich ermöglicht die Implementierung, dass Passwortänderungen nur auf Anwendungsebene vorgenommen werden, wodurch weniger Zurücksetzungen erforderlich sind. Dies reduziert die Wahrscheinlichkeit von gleichen Passwörtern und verhindert dadurch den Bedarf an administrativem Support für Passwort-Resets, wodurch Zeit- und Kostenaufwände vermieden werden können. Durch die Implementierung kann den Nutzern ein sicherer und bequemer Zugriff gewährleistet und die Kosten gesenkt werden. Die Einsicht erfolgt in der Kostenplanung im Kapitel 3.4.

### 3.5.1 Ablaufplanung und Meilensteine

Die Ablaufplanung ist mit einem Gantt-Diagramm und Meilensteine im Kapitel A.1 des Anhangs dargestellt. Dabei stellt die Farbe pink *keine Arbeitszeit*, die Farbe grün eine *reine Arbeitszeit* von 8 Stunden am Tag und die hellblaue Farbe einen *halben Arbeitstag* von 4 Stunden dar. Die jeweiligen Phasen werden mit Meilensteinen abgeschlossen. Die erste Phase startet am Mittwoch, den 01.11.2023, während die letzte mit ihrem Meilenstein am 08.11.2023 endet. Dabei erfolgt die reguläre Arbeitszeit in einer normalen Arbeitswoche von Montag bis Freitag.

### 3.6 Amortisationsdauer

Die Amortisation beschleunigt sich durch die Verwendung von Docker, GitLab und Authentik. Grund dafür ist, dass diese Plattformen Open-Source sind und kostenlos genutzt werden können, was zu einer Reduzierung der Gesamtbetriebskosten (Total Cost of Ownerships (TCO)) führt, da Lizenzkosten eingespart werden können. Eine Zeitersparnis entsteht durch das nicht wiederholte Eingeben der Benutzerdaten, zumal sich durch Authentik nur einmal eingeloggt werden muss und dadurch ein Zugriff auf alle Applikationen erfolgt.

Bei der Einsparung von einer Minute am Tag für jeden der 7 Anwender, nach der dualen Ausbildung und/ oder dem Studium und 220 Arbeitstagen im Jahr, ergibt sich eine gesamte Zeiteinsparung von

$$7 \cdot 220 \text{ Tage/Jahr} \cdot 1 \text{ min/Tag} = 1540 \text{ min/Jahr} \approx 25,67 \text{ h/Jahr} \quad (4)$$

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## 3 Projektplanung

---

Die 40 € wird der Pauschalbetrag für alle Projektmitarbeiter sein.

Die Amortisationszeit setzt sich aus der Division der Gesamtkosten des Projektes und der jährlichen Einsparung zusammen.

$$\frac{1.264,68 \text{ €}}{1.411,85 \text{ €}/\text{Jahr}} \approx 0,90 \text{ Jahre} \approx 47 \text{ Wochen.}$$

Dadurch ergibt sich eine jährliche Einsparung von

$$25,67 \text{ h} \cdot (40 + 15) \text{ €/h} = 1.411,85 \text{ €} \quad (5)$$

## 3.7 Nicht-monetärer Nutzen

Für das Projekt werden die Produkte Authelia, Authentik, Microsoft Azure AD und Sitecar, zur Implementierung in Erwägung gezogen. Wobei mittels einer Nutzwertanalyse, welche im Kapitel 3.2: Authentifizierungs-Tool zu sehen ist, der Sachverhalt durch eine Entscheidungsmatrix dargestellt wird.

Da die Ergebnisse der Wirtschaftlichkeitsanalyse bereits eine ausreichende Begründung für die Umsetzung des Projekts bieten, ist es an dieser Stelle nicht notwendig, eine eingehende Untersuchung der nicht-monetären Vorteile vorzunehmen.

Ohne der Einführung eines Authentifizierungs-Tools wird die Sicherheit der angebotenen Dienste nicht geboten und das Risiko des Datenverlustes gewährleistet. Um das Risiko zu minimieren, soll durch die Nutzwertanalyse ein Ergebnis und die Entscheidungsfindung der jeweiligen Authentifizierungsmethode erleichtert werden.

## 3.8 Abweichungen vom Projektantrag

Die im Projektantrag mit in *Auflage genehmigten* Inhalte, erfordern Änderungen in der Projektdurchführung und -dokumentation.

Erforderliche Änderungen:

- gesamte Zeitplanung - von 35 auf 40 Stunden gestreckt

Folgen der Zeitänderungen:

- Stundenplanung - Planungsphase von 5 auf 8 Stunden
- Stundenplanung - Implementierungsphase von 14 auf 16 Stunden
- Stundenplanung - Testphase von 6 auf 4 Stunden
- Stundenplanung - Dokumentation von 8 auf 6 Stunden
- Zeitplanung/ Planungsphase - *Klärung der Projektziele* nach *vorn* der Phase geschoben
- Zeitplanung/ Dokumentation - *Benutzerdokumentation* statt Entwicklerdokumentation

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## 4 Projektdurchführung

---

Nicht erforderliche Änderungen:

- Implementierungsphase/ Installation und Konfiguration von Sitecars - *Authentik* statt Sitecars

Eine genaue Schilderung, weshalb sich für Authentik anstatt Sitecars entschieden wurde, befindet sich im Kapitel 3.2 Authentifizierungs-Tool

## 3.9 Entwicklungsprozess

Das Projekt unterteilt sich in einem überschaubaren, zeitlich und inhaltlich begrenzten Entwicklungsprozess mit gesondert eingeteilten Phasen, die nach- und voneinander aufbauen. So wird eine Sicherstellung der Schritt- für Schritt-Fertigstellung der jeweiligen Phasen und Übersicht garantiert. Die klaren und umfassend definierten Anforderungen des Projekts ermöglichen eine strukturierte Herangehensweise, die auf vorhersehbaren Bedingungen basiert und einen geradlinigen Fortschritt gewährleistet. Auch ist der Umfang des Projektes zeitlich eingegrenzt und besitzt eine strukturierte Vorgehensweise mit einer geringen Interaktion zum und mit dem Entwicklerteam und des Projektleiters als Kunden.

# 4 Projektdurchführung

## 4.1 Vorbereitung der Entwicklungsumgebung

Die Voraussetzung zur Implementierung von Authentik ist, dass Docker und Docker Compose auf allen Linux-Umgebungen der Instanzen installiert sind, was schon der Fall ist, und über einen Zugang zum Internet verfügen. Die Installation ist erforderlich, da die Conatinerisierung der MFA-Lösung nicht wahrgenommen werden kann. Des Weiteren sollten die zu benötigenden Hard- und Softwarekomponenten, welche ebenfalls in der Sachmittelplanung auf der Seite 7 gelistet sind, funktional sein. Wichtig für die Durchführung ist der Besitz einer Domain oder Subdomain, welche bei der Deloitte Wirtschaftsprüfungsgesellschaft GmbH, aus Datenschutz-Gründen die **domain.de** ist. Die eigentliche Domain der Deloitte wird mit der *example.domain.de* und später der *auth.example.domain.de* ersetzt. Diese muss entweder mit einem A- oder CNAME-Record versehen sein. Mit einem A-Record wird eine Domain oder Subdomain an eine IP-Adresse weitergeleitet und gehört zu den wichtigsten Arten von DNS-Einträgen. Der CNAME-Record hingegen definiert einen Alias für einen anderen DNS-Record und ist im Grunde eine Alternativbezeichnung einer Domain und bedeutet in deutsch so viel wie autorisierte Name. Um die Domain-Namen übersichtlich verwalten zu können, Anschließend wird ein E-Mail Server benötigt, um beispielsweise das Zurücksetzung eines Passworts zu ermöglichen. Für das Testen der kommenden Schritte im Kapitel 4.7 Einrichtung des zweiten Faktors ab der Seite 14 wird das iPhone 12, erwähnt in der Sachmittelplanung, verwendet. Dieses mobile Endgerät ist ein Firmentelefon und beinhaltet den installierten und schon eingerichteten Microsoft Authenticator.

## IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

### 4 Projektdurchführung

---

#### 4.2 Auswahl einer MFA-Lösung

Bei Authentik werden die drei Optionen **WebAuthn Authenticator Setup Stage**, **Static Authenticator Stage** und **TOTP Authenticator Setup Stage** angeboten.

Das Ergebnis der Tabelle 5 Nutzwertanalyse zur MFA-Lösung ist nicht eindeutig zuordbar, bedingt dessen, dass die Optionen WebAuthn Authenticator Setup Stage und TOTP Authenticator Setup Stage um 0,05 Wertungspunkte auseinander liegen und die Entscheidung des finalen Ergebnisses nicht anhand der Nutzwertanalyse zur MFA-Lösung manifestierend festzulegen ist. Die Entscheidung wurde maßgeblich durch die Tatsache beeinflusst, dass die Deloitte Wirtschafts-

Eigenschaft	Wertung	WebAuthn	Static	TOTP
Implementierungsaufwand (niedrig)	25	12	25	18
Zeitersparnis Eingabe	20	14	16	15
Sicherheit	35	35	25	30
Benutzerakzeptanz	20	18	15	18
<b>Gesamt:</b>	<b>100</b>	<b>79</b>	<b>81</b>	<b>81</b>
<b>Nutzwert:</b>		<b>21,65</b>	<b>21,2</b>	<b>21,6</b>

Tabelle 5: Nutzwertanalyse zur MFA-Lösung

prüfungsgesellschaft GmbH das TOTP-Verfahren für sämtliche verfügbaren Dienste einsetzt. Dieses Verfahren erfordert die Eingabe eines einmaligen Passworts über einen Authenticator, wie es beim iPhone 12 der Fall ist. Daraufhin fiel die Entscheidung auf das **TOTP-Verfahren**, welches hingegen zum WebAuthn Authenticator Setup Stage weniger Sicherheit aber weniger Implementierungsaufwand erfordert und kein weiteres Gerät oder eine Software notwendig ist. In dem TOTP Authenticator Setup Stage geben alle Benutzer zu Beginn ihren Nutzernamen und das zugehörige Passwort ein. Nach einer erfolgreichen Anmeldung, werden die Benutzer anschließend weitergeleitet, um einen 6-stelligen Zahlencode einzugeben. Dieser Code ist in dem Microsoft Authenticator für 30 Sekunden sichtbar. Wenn die Benutzer sich noch nicht über Authentik angemeldet hatten, werden diese nach der Anmeldung aufgefordert, einen QR-Code mit dem Microsoft Authenticator abzuscannen, wodurch der 6-stellige Code generiert wird. Dieser ist daraufhin, wie oben beschrieben, bei jeder Anmeldung einzugeben.

#### 4.3 Erstellung der docker-compose.yml und .env

Um Authentik über eine *docker-compose.yml*-Datei lauffähig zu machen, müssen der Authentik-Server, der Authentik-Worker, Redis und PostgreSQL gleichzeitig erstellt werden, was durch die Docker-Containersierung geschieht. PostgreSQL ist eine objektrelationale Datenbank und unterstützt die Erweiter- und Skalierbarkeit der Cloud-Infrastruktur. Redis hingegen ist ein In-Memory-Datenspeicher, der als schneller Datenspeicher dient. Die ".env"-Datei im Kapitel A.7 .env enthält die individuellen Umgebungsvariablen für die Zugangsdaten der Nutzern. Eine Darstellung der Instanzen befindet sich im Kapitel A.5 Cloud-Infrastruktur. Die "docker-compose.yml"-Datei wurde über [COMPOSERIZE \[2023\]](#), einer Applikation aus dem Internet

## IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

### 4 Projektdurchführung

---

entnommen, welche öffentlich zugänglich ist. Auch die ”.env”-Datei ist öffentlich über die Webpage von Authentik einsehbar. Mittels Composerize ist es möglich anstatt eines Docker-Befehls, eine docker-compose.yml-Datei zu erstellen.

Die einzigen in dieser Datei vorzunehmenden Änderungen, sind die Variablen *pg\_pass*, *authentik\_secret\_key*, *authentik\_email\_host*, *authentik\_email\_username*, *authentik\_host\_password* und *authentik\_email\_from*. Um Authentik zu starten, werden beide Dateien im Unterordner Authentik eingefügt. Der Befehl **docker-compose pull** lädt die Konfigurationen und Dienste gemäß der Angaben in der **docker-compose.yml** herunter. Dabei werden die benötigten Abhängigkeiten und Einstellungen für Container in Docker-Images abgerufen, während Docker-Volumes dafür sorgen, dass Daten persistent bleiben, selbst wenn Container gelöscht werden. Anschließend, durch die Ausführung von **docker-compose up -d**, wird sichergestellt, dass die docker-compose.yml-Datei vorhanden ist und startet die Container für die definierten Dienste im Hintergrund mithilfe des Parameters **-d** (**--detach**). Nach dem Start der Container kann ihr Status mittels **docker-compose ps** überprüft werden. Weitere Einzelheiten und Ergebnisse dieser Befehle findest du im Anhang (A.8) Docker-Befehle.

#### 4.4 Konfiguration des NGinx Reverse Proxy Managers

Nachdem Authentik in einem Docker-Container läuft, erfolgt die Konfiguration des NGinx Reverse Proxy Managers:

1. Erstellung einer Authentifizierungs-Domain (auth.example.domain) und Einstellung eines A-Records im DNS-Resolver
2. Im NGinx Reverse Proxy Managers einen neuen Host erstellen, was im Anhang in der A.9 Proxy Host Konfiguration einsehbar ist
3. private IP-Adresse des Authentik-Servers mit der in der .env-Datei eingegebenen Portnummer (80) eingeben mit dem Resultat für das Beispiel: **0.0.0.0:80** - Einsicht im A.9 Proxy Host Konfiguration
4. im SSL-Tab des Konfigurationsfeldes, anklicken: *Force SSL, HTTP/2 Support, HSTS Enabled* und *HSTS Subdomains*
5. im E-Mail Feld die E-Mail Adresse (admin@example.domain.de) eingeben und den Nutzungsbedingungen zustimmen
6. Ergebnis: Zugriff auf Authentik möglich, sodass die Willkommens-Seite sichtbar wird, welche im Anhang im Kapitel A.9 Proxy Host Konfiguration einsehbar ist

## IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

### 4 Projektdurchführung

---

#### 4.5 Konfiguration von Authentik

Nach der Konfiguration des NGinx Reverse Proxy Managers, werden in Authentik ein Projekt und die vorhandenen User erstellt. Diese Vorgehensweise ist im Anhang in der A.10 Authentik-Konfiguration detailliert beschrieben.

Grobe Vorgehensweise:

1. Einrichtung eines Projektes
2. Erstellung von Benutzern
3. Hinzufügen des NGinx Proxy Managers
4. Einrichtung des zweiten Faktors erfolgt in Kapitel 4.7 auf der Seite 14

#### 4.6 Integration mit Cloud-Diensten

Damit sich Authentik vor jeden Dienst in der gegebenen Cloud-Infrastruktur schalten kann, wird in der Host-Konfiguration im NGinx Reverse Proxy Manager im Bereich *Advanced* die im Anhang erwähnte NGinx Konfiguration eingefügt. Wobei zu beachten ist, dass bei jedem Dienst die Portnummer geändert werden muss, sodass eine Umleitung von Authentik auf diesen erfolgen kann.

#### 4.7 Einrichtung des zweiten Faktors

Nach dem Ergebnis aus der Nutzwertanalyse zur MFA-Lösung im Kapitel 4.2 Auswahl einer MFA-Lösung geht das TOTP-Verfahren hervor. Ein Auszug der TOTP-Einrichtung im Anhang zeigt die Konfiguration des zweiten Faktors.

Ein kurze Schrittfolge zur Einrichtung dieses:

1. Login bei Authentik
2. auf **Einstellungen** gehen und **MFA Devices** bestätigen
3. **Enroll** bestätigen - eine Methode auswählen:
  - WebAuth Authenticator Setup Stage
  - Static Authenticator Stage
  - *TOTP Authenticator Setup Stage* - auswählen
4. Logout bei Authentik
5. erneut Login - QR-Code mit dem Microsoft Authenticator scannen
6. 6-stelligen Code eingeben und einloggen

## IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

### 5 Test- und Abnahme

---

## 4.8 Maßnahmen zur Qualitätssicherung

### 4.8.1 Produktorientierte Maßnahmen

Die produktorientierten Maßnahmen konzentrieren sich auf die Sicherstellung der Qualität des MFAs. Dazu gehören die vorzunehmenden Zugriffstests, dargestellt durch Black- und Whitebox-Tests, die die Anforderungen überprüfen und im Anhang A.14 Testprotokoll einsehbar sind. Um die Anforderungen zu erfüllen, erfolgten die Tests so, dass Birk Spinn und Edgar Johann Kapler ein Feedback auf Korrektheit abgeben werden.

### 4.8.2 Prozessorientierte Maßnahmen

Während der Fokus der prozessorientierten Maßnahmen auf der Qualitätssicherung im Rahmen der Prozesse und Abläufe liegt, die zur Implementierung von Authentik gehören. Durch die kontinuierliche Anwendung des Qualitätsmanagementsystems gemäß ISO 9001 im Qualitätsmanagement erfolgt nach der Planung eine sorgfältige Überprüfung jedes Schrittes auf Richtigkeit. Bei festgestellten Fehlern wird nach alternativen Wegen zur Zielerreichung gesucht, um diese erfolgreich umzusetzen. Dieser Prozess folgt nach dem [PDCA-ZYKLUS \[2023\]](#)-Zyklus.

Als Online-Dienstleister ist es laut den Vorschriften des Bundesamts für Sicherheit in der Informationstechnik (BSI) zwingend erforderlich, Daten und Geräte durch eine Mehrfaktor-Authentifizierung (MFA) zu schützen, bei der der Login durch die Verwendung eines Passworts und eines weiteren Faktors abgesichert wird. Authentik, als Identitätsprovider, nutzt ein Informationssicherheitssystem, das auf etablierten Standards wie BSI100-2 und ISO27001 basiert und die Anforderungen erfüllt. Der Standard BSI 100-2 ist ein Standard des Bundesamtes für Sicherheit in der Informationstechnik, der allgemeine Anforderungen an eine Managementsystem für Informationssicherheit (ISMS) definiert. Die ISO 27001 ist eine internationale Norm für ISMS und ist auf der Basis von IT-Grundschutz für die Standard-Absicherung, als auch für die Kern-Absicherung möglich.

## 5 Test- und Abnahme

### 5.1 Überwachung der Laufzeit der Dienste

Die Überwachung der Laufzeit der eingetragenen Dienste passiert über das Dashboard von Authentik.

Um jeden einzelnen Dienst schlussendlich zu überprüfen, erfolgte über den NGinx Reverse Proxy Manager ein jeweiliger Zugriff auf alle Dienste, um zu testen, ob sich Authentik auch wirklich vor den Dienst schaltet. Zusätzlich wird das Monitoring-Tool Uptime Kuma verwendet, um die Laufzeit aller Dienste zu überprüfen.

## **IMPLEMENTIERUNG VON MFA**

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## *6 Dokumentation*

---

### **5.2 Überprüfung/ Beseitigung von Fehlern**

Nach der erfolgreichen Durchführung des Projektes wurden die funktionalen und nicht-funktionalen Anforderungen aus der Anforderungsanalyse ebenfalls durch den Manager Edgar Johann Kapler und dualen Studenten Birk Spinn getestet. Das Beseitigen von Fehlern in der Entwicklungs-umgebung erfolgte während der Durchführungsphase mittels des Plan-Do-Check-Act-Zyklus, in welchem die Fehler, z. B. Tippfehler gleich während der Implementierung behoben wurden. Aufgrund dieser Vorgehensweise ist ein kontinuierlicher Verbesserungsprozess garantiert.

### **5.3 Zugriffstests**

Um den Zugriff zu testen, wurden **BLACKBOX UND WHITEBOX [2023]**-Tests durchgeführt, die Authentik auf die Gesamtheit überprüfen und sicherstellen, dass die Benutzeranmeldungen und Authentifizierungen erfolgreich verlaufen. Dabei agieren Blackbox-Test-Tester gewissermaßen im Ungewissen, da sie keine Einsicht in die interne Funktionsweise des Systems haben. Dies kann dazu führen, dass sie während des Tests auf unerwartete Probleme stoßen. Sie wissen nicht, wie eine Software funktioniert, wie sie implementiert ist oder aus welchen Komponenten sie besteht. In einem White-Box Test haben die Testpersonen Kenntnisse des Codes und der Funktionsweisen der Software. Die Einsicht in die Ergebnisse des Testprotokolls sind im Anhang A.14 Testprotokoll einsehbar.

### **5.4 Abnahme**

Die Abnahme verlief reibungslos, wodurch das Projekt am 8. November 2023 erfolgreich an Edgar Johann Kapler übergeben und anschließend in der Produktivumgebung erfolgreich umgesetzt werden konnte.

## **6 Dokumentation**

### **6.1 Benutzerdokumentation**

Die Benutzerdokumentation befindet sich im Anhang A.13 Benutzerdokumentation. Darin befindet sich eine kurze Schilderung über den Login bei Authentik mit TOTP.

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## 7 Fazit

---

### 7 Fazit

#### 7.1 Soll-/Ist-Vergleich

Das Projektziel wurde erfolgreich innerhalb des vorgegebenen Zeitrahmens erreicht. Während der Planung stellte sich jedoch heraus, dass die geschätzte Dauer der Testphase von ursprünglich 4 Stunden zu grob war und stattdessen in 3 Arbeitsstunden abgeschlossen wurde. Daher wurde die übrige 1 Stunde zur Verbesserung der Dokumentation verwendet. Die geplanten Arbeitsstunden für die beiden beteiligten Teammitglieder wurden voll ausgeschöpft, und die Ressourcen, wie in der Sachmittelplanung beschrieben, effizient genutzt.

Wie in Tabelle 6 Soll-/Ist-Vergleich zu erkennen ist, konnte die Zeitplanung bis auf wenige Ausnahmen eingehalten werden.

Phase	Geplant	Tatsächlich	Differenz
Planungsphase	8 h	8 h	h
Implementierungsphase	16 h	16 h	
Testphase	4 h	3 h	-1 h
Einführung und Übergabe	4 h	4 h	
Dokumentation	8 h	9 h	+1 h
<b>Gesamt</b>	<b>40 h</b>	<b>40 h</b>	

Tabelle 6: Soll-/Ist-Vergleich

#### 7.2 Gewonnene Erkenntnisse

Die Zeitplaung und Schätzung der Testphase erwies sich als grob und ungenau. Es ist wichtig zu beachten, realistische Zeitpläne zu erstellen und eventuell genügend Puffer einzukalkulieren. Bedingt dessen, dass die Dokumentation ein integraler Bestandteil der Projektarbeit ist, wurde die verkürzte Zeit für die Testphase sinnvoll für die Verbesserung der Inhalte in der Dokumentation genutzt. Ein Vorteil der ausgewählten MFA-Lösung ist, dass die Implementierung recht schnell und nachvollziehbar ging.

#### 7.3 Ausblick

Das Projekt ist eine Tochterprojekt eines übergeordneten Projektes. Mit dem Ergebnis wird die Sicherheit der vorhandenen Dienste gewährleistet bzw. verbessert. Authentik als Identitäts-Provider wird erweitert, um die Entwicklung eines Unternehmensdesigns zu ermöglichen. Außerdem werden Monitoring-Alerts integriert, um bei fehlerhaften Logins oder Logouts automatisch Benachrichtigungen per E-Mail zu versenden.

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

*A Anhang*

---

## **A Anhang**

### **Abkürzungsverzeichnis**

<b>SSH</b>	Secure Shell
<b>B and TCL</b>	Business & Technology Center Leipzig
<b>API</b>	Application Programming Interface
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>OIDC</b>	OpenID Connect
<b>CPU</b>	Control Processing Unit
<b>RAM</b>	Random Access Memory
<b>CLI</b>	Command Line Interface
<b>A</b>	Adresse
<b>CNAME</b>	Canonical name
<b>DNS</b>	Domain Name System
<b>HSTS</b>	HTTP Strict Transport Security
<b>ISMS</b>	Informationssicherheits-Managementsystem
<b>BSI</b>	Bundesamt für Sicherheit in der Informationstechnik
<b>TOTP</b>	Time-based One-time Password
<b>SSO</b>	Single-Sign On
<b>MFA</b>	Multi Faktor Authentifizierung
<b>IDE</b>	Integrated Development Environment
<b>TCO</b>	Total Cost of Ownership

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## A Anhang

---

### Begriffserklärung

**SSH** Secure Shell - Netzwerkprotokoll zur sicheren Datenübertragung

**B and TCL** Business & Technology Center Leipzig - Deloitte Standort in Leipzig

**API** Application Programming Interface - Schnittstelle zur Kommunikation zwischen Softwareanwendungen

**LDAP** Lightweight Directory Access Protocol - Protokoll zum Abrufen von Informationen aus einem Verzeichnisdienst

**OIDC** OpenID Connect - Authentifizierungsprotokoll für Webanwendungen

**CPU** Control Processing Unit - zentrale Recheneinheit eines Computers

**RAM** Random Access Memory - Speichertyp, der Daten temporär speichert und schnell darauf zugreifen kann

**CLI** Command Line Interface - textbasierte Benutzeroberfläche zur Interaktion mit einem Computersystem

**A** Address (DNS Resource Record) - DNS-Ressourceneintrag, der eine IPv4-Adresse mit einem Domainnamen verknüpft

**CNAME** Canonical name - Eintrag in DNS, der eine Alias-Beziehung zwischen zwei Domainnamen darstellt

**DNS** Domain Name System - System zur Übersetzung von Domainnamen in IP-Adressen

**HSTS** HTTP Strict Transport Security - Sicherheitsmechanismus, der Webanwendungen vor bestimmten Angriffen schützt

**ISMS** Informationssicherheits-Managementsystem - Rahmenwerk zur Informationssicherheit in Organisationen

**BSI** Bundesamt für Sicherheit in der Informationstechnik - deutsche Behörde für IT-Sicherheit

**TOTP** Time-based One-time Password - Einmalpasswort, das basierend auf der Zeit generiert wird

**SSO** Single-Sign On - Authentifizierungsverfahren, bei dem sich Benutzer einmal anmelden, um auf verschiedene Dienste zuzugreifen

**MFA** Multi Faktor Authentifizierung - Authentifizierungsverfahren, das mehrere Methoden zur Bestätigung der Identität eines Benutzers verwendet

**IDE** Integrated Development Environment - intelligente Entwicklungsumgebung für die Softwareentwicklung

**TCO** Total Cost of Ownership - Gesamtkosten von Produktanschaffung und Nutzung

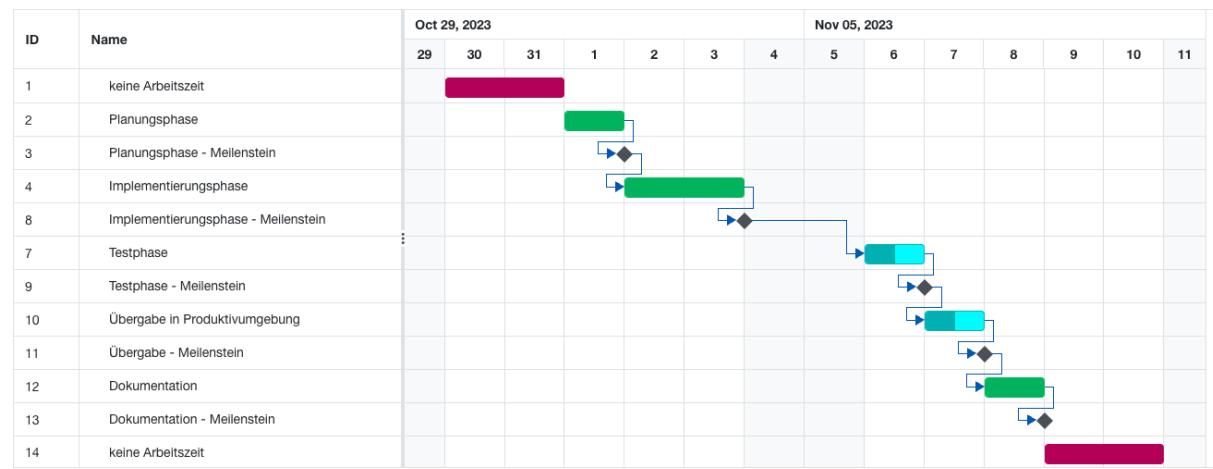
# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## A Anhang

---

### A.1 Gantt-Diagramm und Meilensteine



# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## A Anhang

### A.2 Detaillierte Zeitplanung

<b>1. Problemstellung</b>	<b>0.5 h</b>
<b>2. Ist-/Soll-Analyse</b>	<b>5.5 h</b>
2.1 Projektumfeld	1 h
2.2 Projektaufgabe	0.5 h
2.3 Projektziel	0.5 h
2.4 Projektschnittstellen	2 h
2.5 Anforderungsanalyse	1.5 h
<b>3. Projektplanung</b>	<b>7 h</b>
3.1 Projektphasen	0.5 h
3.2 Authentifizierungs-Tool	1 h
3.3 Ressourcenplanung	1.5 h
3.4 Kostenplanung	0.5 h
3.5 Wirtschaftlichkeitsanalyse	0.5 h
3.6 Amortisationsdauer	1.5 h
3.7 Nicht-monetärer Nutzen	0.5 h
3.8 Abweichungen vom Projektantrag	0.5 h
3.9 Entwicklungsprozess	1 h
<b>4. Projektdurchführung</b>	<b>12 h</b>
4.1 Vorbereitung der Entwicklungsumgebung	2 h
4.2 Auswahl MFA-Lösung	1 h
4.3 Erstellung der docker-compose.yml und .env	3 h
4.4 Konfiguration des NGinx Reverse Proxy Managers	2 h
4.5 Konfiguration von Authentik	2 h
4.6 Integration mit Cloud-Diensten	1 h
4.7 Einrichtung des zweiten Faktors	1 h
4.8 Maßnahmen zur Qualitätssicherung	1 h
<b>5. Test- und Abnahme</b>	<b>3 h</b>
5.1 Überwachung der Laufzeit der Dienste	1 h
5.2 Überprüfung/ Beseitigung von Fehlern	1 h
5.3 Zugriffstests	1 h
<b>6. Dokumentation</b>	<b>8 h</b>
6.1 Dokumentation	7 h
6.2 Benutzerdokumentation	1 h
<b>6. Fazit</b>	<b>4 h</b>
7.1 Soll-/ Ist-Vergleich	2.5 h
7.2 Gewonnene Erkenntnis	1 h
7.3 Ausblick	0.5 h
<b>Gesamt</b>	<b>40 h</b>

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

A Anhang

## A.3 Use Case-Diagramm

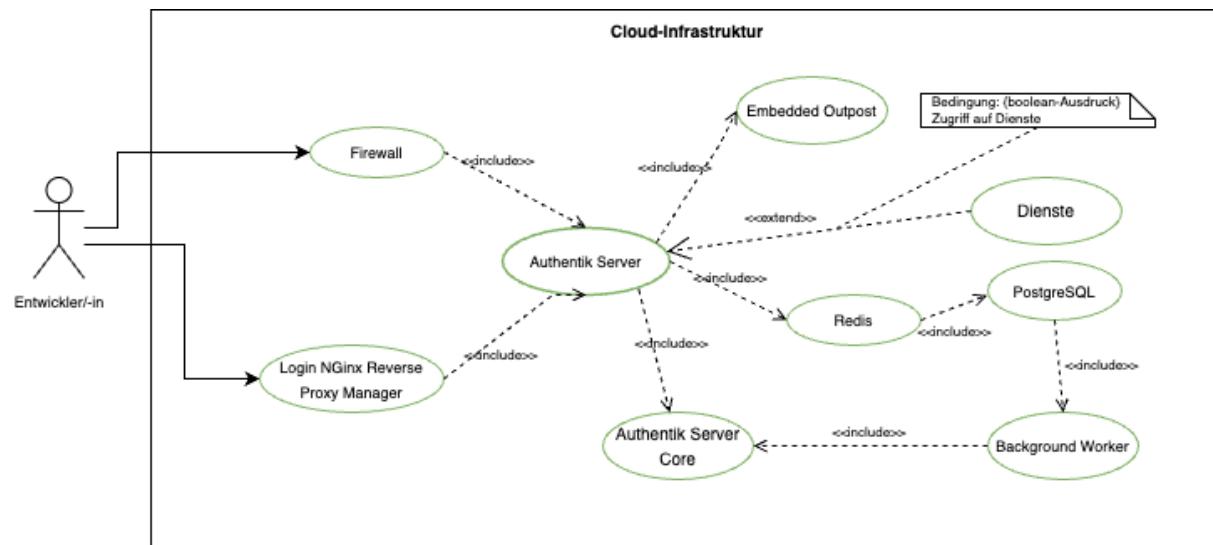


Abbildung 1: Use Case-Diagramm

## IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

### A Anhang

#### A.4 Sequenzdiagramm CLI Zugriff auf die Instanzen

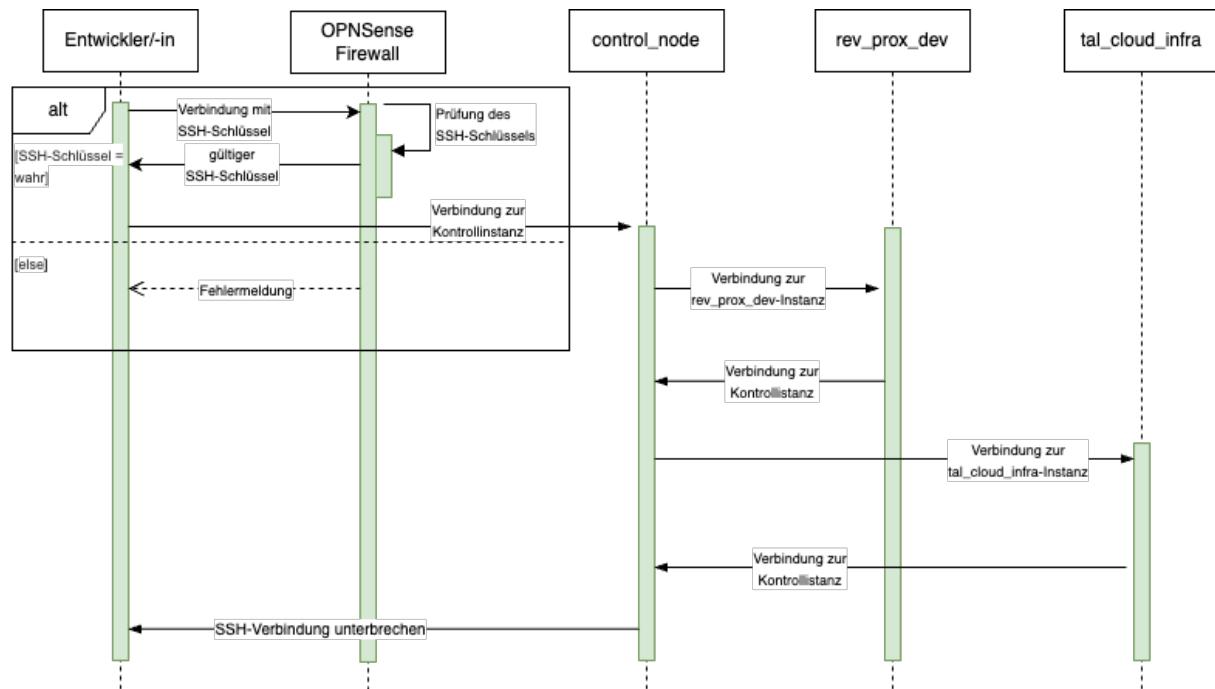


Abbildung 2: Sequenzdiagramm

## IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

A Anhang

---

### A.5 Cloud-Infrastruktur

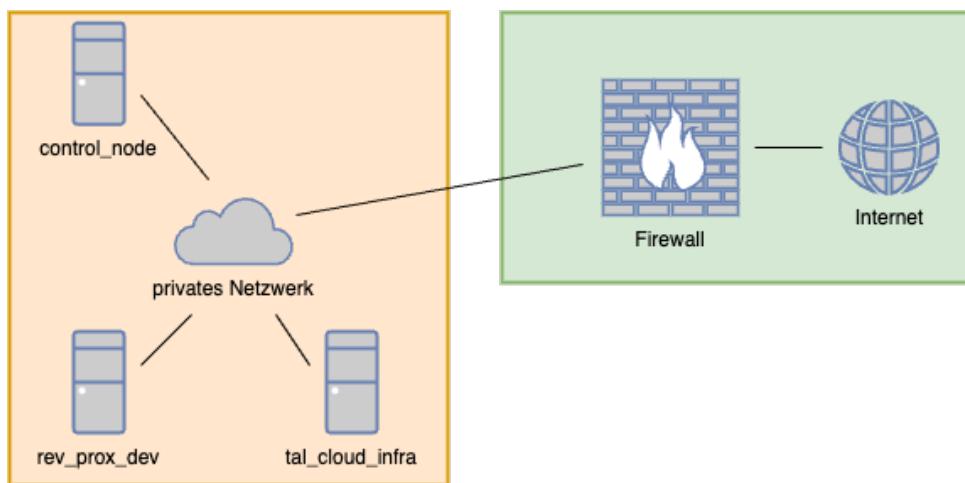


Abbildung 3: Cloud-Infrastruktur

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## A Anhang

### A.6 docker-compose.yml

```
version: "3.4"

services:
  postgresql:
    image: docker.io/library/postgres:12-alpine
    restart: unless-stopped
    healthcheck:
      test: ["CMD-SHELL", "pg_isready -d ${POSTGRES_DB} -U ${POSTGRES_USER}"]
    start_period: 20s
    interval: 30s
    retries: 5
    timeout: 5s
    volumes:
      - ./database:/var/lib/postgresql/data
    environment:
      POSTGRES_PASSWORD: ${PG_PASS}:?database password required)
      POSTGRES_USER: ${PG_USER:-authentik}
      POSTGRES_DB: ${PG_DB:-authentik}
    env_file:
      - .env
  redis:
    image: docker.io/library/redis:alpine
    command: --save 60 1 --loglevel warning
    restart: unless-stopped
    healthcheck:
      test: ["CMD-SHELL", "redis-cli ping | grep PONG"]
    start_period: 20s
    interval: 30s
    retries: 5
    timeout: 3s
    volumes:
      - ./redis:/data
  server:
    image: ${AUTHENTIK_IMAGE:-ghcr.io/goauthentik/server}:${AUTHENTIK_TAG:-2023.8.3}
    restart: unless-stopped
    command: server
    environment:
      AUTHENTIK_REDIS_HOST: redis
      AUTHENTIK_POSTGRESQL_HOST: postgresql
      AUTHENTIK_POSTGRESQL_USER: ${PG_USER:-authentik}
      AUTHENTIK_POSTGRESQL_NAME: ${PG_DB:-authentik}
      AUTHENTIK_POSTGRESQL_PASSWORD: ${PG_PASS}
    volumes:
      - ./media:/media
      - ./custom-templates:/templates
    env_file:
      - .env
    ports:
      - "${COMPOSE_PORT_HTTP:-9000}:9000"
      - "${COMPOSE_PORT_HTTPS:-9443}:9443"
    depends_on:
      - postgresql
      - redis
  workers:
    image: ${AUTHENTIK_IMAGE:-ghcr.io/goauthentik/server}:${AUTHENTIK_TAG:-2023.8.3}
    restart: unless-stopped
    command: worker
    environment:
      AUTHENTIK_REDIS_HOST: redis
      AUTHENTIK_POSTGRESQL_HOST: postgresql
      AUTHENTIK_POSTGRESQL_USER: ${PG_USER:-authentik}
      AUTHENTIK_POSTGRESQL_NAME: ${PG_DB:-authentik}
      AUTHENTIK_POSTGRESQL_PASSWORD: ${PG_PASS}
    # `user: root` and the docker socket volume are optional.
    # See more for the docker socket integration here:
    # https://goauthentik.io/docs/outposts/integrations/docker
    # Removing `user: root` also prevents the worker from fixing the permissions
    # on the mounted folders, so when removing this make sure the folders have the correct UID/GID
    # (1000:1000 by default)
    user: root
    volumes:
      - /var/run/docker.sock:/var/run/docker.sock
      - ./media:/media
      - ./certs:/certs
      - ./custom-templates:/templates
    env_file:
      - .env
    depends_on:
      - postgresql
      - redis
  volumes:
    database:
      driver: local
    redis:
      driver: local
```

Annotations:

- PostgreSQL wird installiert  
Version 12 wird verwendet  
Container startet sich neu, solange er nicht gestoppt wird
- Tests des Containers, um sicherzustellen, dass er läuft, wie lange er läuft und ab wann wie oft wiederholt wird
- Erstellung eines Speichermediums im Unterordner von Authentik database
- Anforderung der Umgebungsvariablen aus der zu erstellten .env-Datei
- Redis hilft bei der Zwischenspeicherung  
Version alpine wird verwendet  
Befehl: Betrieb von Redis soll aufgenommen werden
- Erstellung des Speichermediums im Unterordner von Authentik redis
- Authentik Server mit dem zu ziehenden Image (Abbildung der spezifischen Version)
- Command: Start des Servers  
Referenzen zu o.g. Redis und PostgreSQL
- Zuordnung der freien Ports für HTTP und HTTPS
- abhängig von postgresql und redis
- Worker entlastet den Hauptserver
- Definition der Volumen (Speichermedien), der inkludierten Datenbank und Reis

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## A Anhang

---

### A.7 .env

```
PG_USER=authentik
PG_PASS=aReallyLongStrongPasswordShouldBePutHere
AUTENTIK_SECRET_KEY=someincrediblylongcomplexkeygoeshere
AUTENTIK_ERROR_REPORTING_ENABLED=true
# SMTP Host Emails are sent to
AUTENTIK_EMAIL_HOST=smtp.example.com
AUTENTIK_EMAIL_PORT=587
# Optionally authenticate (don't add quotation marks to your password)
AUTENTIK_EMAIL_USERNAME=auth@example.com
AUTENTIK_EMAIL_PASSWORD=a-L0n6-Strong_password_should_go_here
# Use StartTLS
AUTENTIK_EMAIL_USE_TLS=true
# Use SSL
AUTENTIK_EMAIL_USE_SSL=false
AUTENTIK_EMAIL_TIMEOUT=10
# Email address authentik will send from, should have a correct @domain
AUTENTIK_EMAIL_FROM=auth@example.com
COMPOSE_PORT_HTTP=80
COMPOSE_PORT_HTTPS=443
# Authentik Version to Full
AUTENTIK_TAG=2023.8.3
```

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## A Anhang

---

### A.8 Docker-Befehle

```
mfa@[REDACTED] Authentik % docker-compose pull
[+] Pulling 4/4
  ✓ server Skipped - Image is already being pulled by worker
  ✓ worker Pulled
  ✓ postgresql Pulled
  ✓ redis Pulled
mfa@[REDACTED] Authentik % docker ps -a
```

Abbildung 4: Docker Pull

```
mfa@[REDACTED] Authentik % sudo docker-compose up -d
Password:
[+] Building 0.0s (0/0)
[+] Running 4/4
  ✓ Container authentik-postgresql-1 Started
  ✓ Container authentik-redis-1 Started
  ✓ Container authentik-worker-1 Started
  ✓ Container authentik-server-1 Started
mfa@[REDACTED] Authentik %
```

Abbildung 5: Docker Compose Up

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## A Anhang

### A.9 Proxy Host Konfiguration

New Proxy Host

Details   Custom locations   SSL   Advanced

Domain Names \*

Scheme \* Forward Hostname / IP \* Forward Port \*

http 0.0.0.0 80

Cache Assets  Block Common Exploits

Websockets Support

Access List

Publicly Accessible

Proxy Host Konfiguration – Details

New Proxy Host

Details   Custom locations   SSL   Advanced

SSL Certificate

Request a new SSL Certificate

Force SSL  HTTP/2 Support

HSTS Enabled  HSTS Subdomains

Use a DNS Challenge

Email Address for Let's Encrypt \*

I Agree to the [Let's Encrypt Terms of Service](#) \*

Proxy Host Konfiguration – SSL

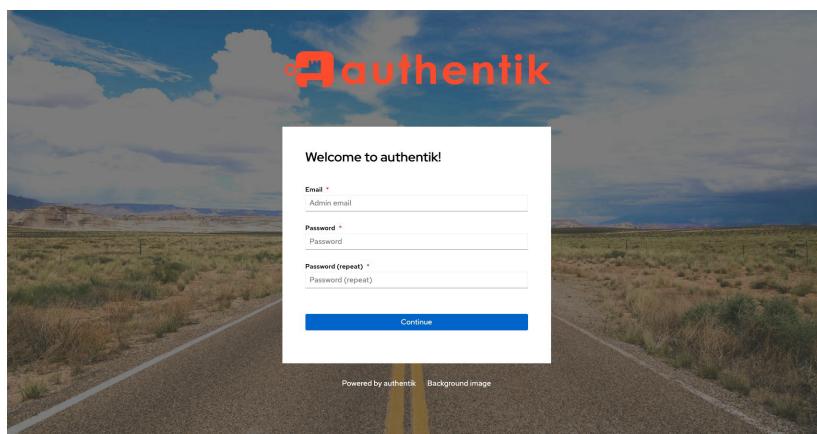
0.0.0.0:8080/if/flow/default-authentication-flow/?next=%2F

Im Webbrowser:  
Startlink (vor der Änderung)

0.0.0.0:8080/if/flow/initial-setup/

<0.0.0.0:8080/if/flow/initial-setup/>

Im Webbrowser:  
Startlink (nach der Änderung)



Authentik - Willkommensseite

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

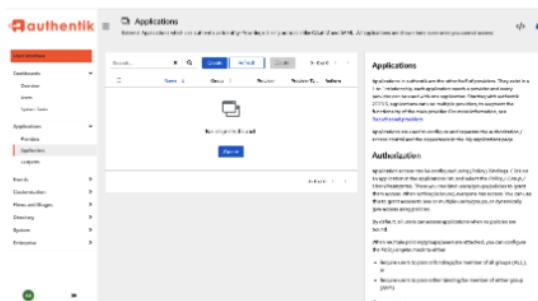
A Anhang

## A.10 Authentik-Konfiguration

### Erstellung einer Application (Anwendung):

Notwendig, um die zu schützenden Anwendungen hinzuzufügen

#### 1. Über Applications – Applications auf Create gehen



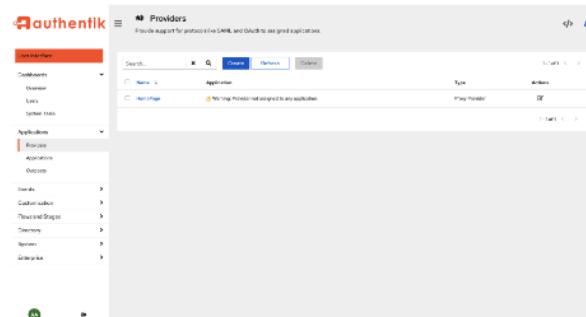
#### 2. Im Create-Modus die jeweiligen Inhalte einfügen

- Aus Demonstrationszwecken wird mit die HomePage als Anwendung genutzt



#### 3. Auf Applications – Providers lässt sich die erstellte Anwendung einsehen

- Noch nicht einsetzbar, da der Provider nicht eingerichtet ist



# IMPLEMENTIERUNG VON MFA

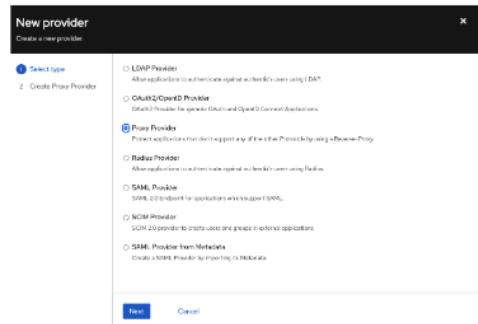
Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## A Anhang

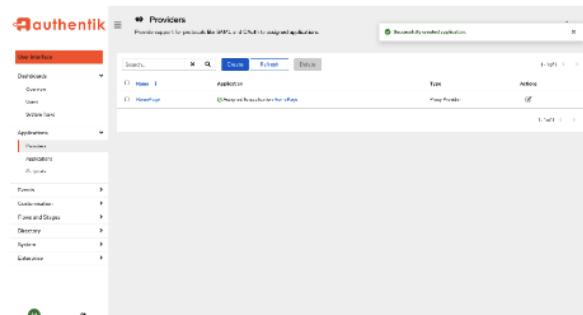
### Einrichten des Providers:

#### 1. Über Applications – Providers, Create einen neuen Provider einrichten

- Das Projekt arbeitet mit dem NGinx Reverse Proxy Manager, sodass der **Proxy Provider** ausgewählt werden muss

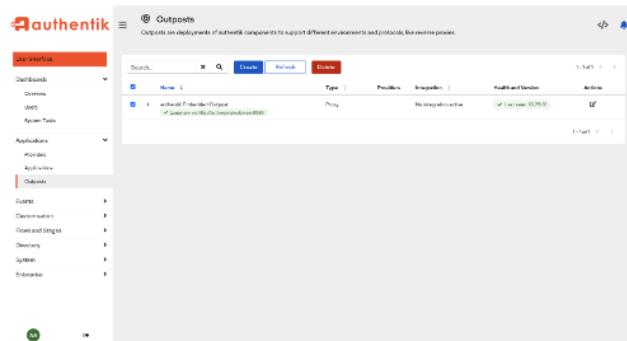


#### 2. Über Applications – Providers ist nun der erstellte Provider für die HomePage einsehbar



#### 3. Über Applications – Outposts werden

- Die Einrichtung eines **Außenpostens** ist notwendig, da dieser unabhängig der Umgebung arbeiten kann



# IMPLEMENTIERUNG VON MFA

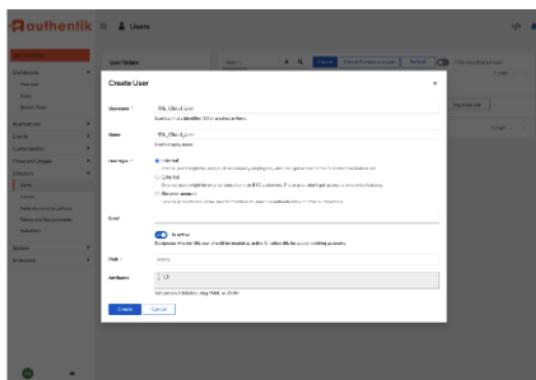
Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## A Anhang

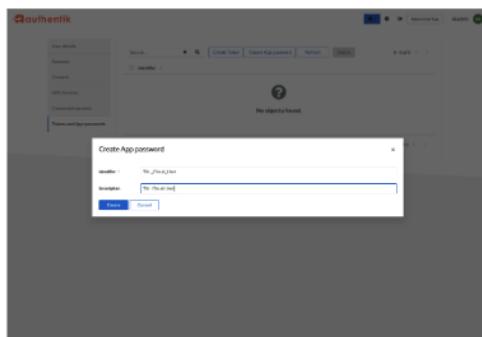
### Einrichtung eines Benutzers:

Zur Zugriffssteuerung und Personalisierung der Nutzerprofile

1. Über *Directory – Users* auf *Create* das Pop-Up -Fenster öffnen



2. Auf *Einstellungen – Tokens and App passwords* ein Passwort für den Benutzer anlegen



3. Ausloggen und testen

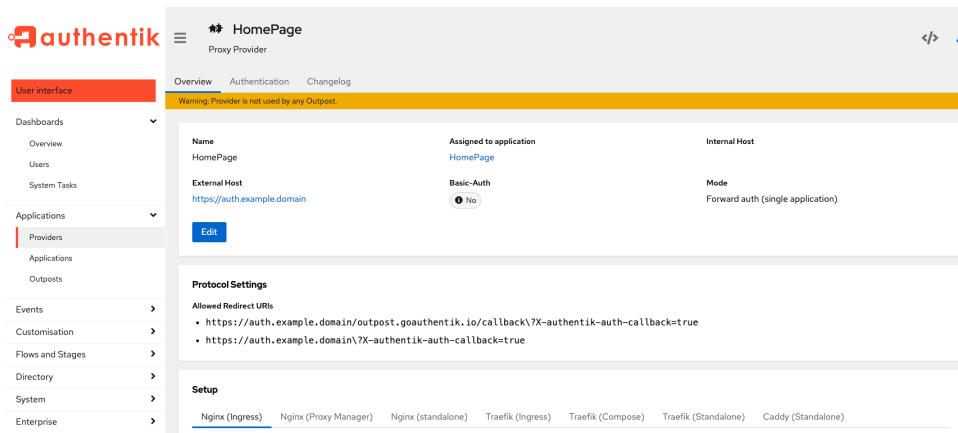


# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## A Anhang

### A.11 NGinx Konfiguration



**Abbildung:**  
Authentik – HomePage (Providers) NGinx Auswahl (Proxy Manager)

Code, der in in der Proxy Host Konfiguration in *Advanced* eingefügt werden muss:

```
# Increase buffer size for large headers
# This is needed only if you get 'upstream sent too big header while reading response
# header from upstream' error when trying to access an application protected by goauthentik
proxy_buffers 8 16k;
proxy_buffer_size 32k;

# Make sure not to redirect traffic to a port 4443
port_in_redirect off;

location / {
    # Put your proxy_pass to your application here
    proxy_pass $forward_scheme://$server:$port;
    # Set any other headers your application might need
    # proxy_set_header Host $host;
    # proxy_set_header ...;

    ##### @authentik-specific config #####
    auth_request /outpost.goauthentik.io/auth/nginx;
    error_page 401 = @goauthentik_proxy_signin;
    auth_request_set $auth_cookie $upstream_http_x_authentik_cookie;
    add_header Set-Cookie $auth_cookie;

    # translate headers from the outposts back to the actual upstream
    auth_request_set $authentik_username $upstream_http_x_authentik_username;
    auth_request_set $authentik_groups $upstream_http_x_authentik_groups;
    auth_request_set $authentik_email $upstream_http_x_authentik_email;
    auth_request_set $authentik_name $upstream_http_x_authentik_name;
    auth_request_set $authentik_uid $upstream_http_x_authentik_uid;

    proxy_set_header X-authentik-username $authentik_username;
    proxy_set_header X-authentik-groups $authentik_groups;
    proxy_set_header X-authentik-email $authentik_email;
    proxy_set_header X-authentik-name $authentik_name;
    proxy_set_header X-authentik-uid $authentik_uid;
}

# all requests to /outpost.goauthentik.io must be accessible without authentication
location /outpost.goauthentik.io {
    proxy_pass http://0.0.0.0:3001/outpost.goauthentik.io;
    # ensure the host of this vserver matches your external URL you've configured
    # in authentik
    proxy_set_header Host $host;
    proxy_set_header X-Original-URL $scheme://$http_host$request_uri;
    add_header Set-Cookie $auth_cookie;
    auth_request_set $auth_cookie $upstream_http_set_cookie;
    proxy_pass_request_body off;
    proxy_set_header Content-Length "";
}

# Special location for when the /auth endpoint returns a 401,
# redirect to the /start URL which initiates SSO
location @goauthentik_proxy_signin {
    internal;
    add_header Set-Cookie $auth_cookie;
    return 302 /outpost.goauthentik.io/start?rd=$request_uri;
    # For domain level, use the below error_page to redirect to your authentik server with the full redirect path
    # return 302 https://authentik.company/outpost.goauthentik.io/start?rd=$scheme://$http_host$request_uri;
}
```

Kommentare im Code:

- # Increase buffer size for large headers
- # This is needed only if you get 'upstream sent too big header while reading response
- # header from upstream' error when trying to access an application protected by goauthentik
- proxy\_buffers 8 16k;
- proxy\_buffer\_size 32k;
- # Make sure not to redirect traffic to a port 4443
- port\_in\_redirect off;
- location / {
- # Put your proxy\_pass to your application here
- proxy\_pass \$forward\_scheme://\$server:\$port;
- # Set any other headers your application might need
- # proxy\_set\_header Host \$host;
- # proxy\_set\_header ...;
- ##### @authentik-specific config #####
- auth\_request /outpost.goauthentik.io/auth/nginx;
- error\_page 401 = @goauthentik\_proxy\_signin;
- auth\_request\_set \$auth\_cookie \$upstream\_http\_x\_authentik\_cookie;
- add\_header Set-Cookie \$auth\_cookie;
- # translate headers from the outposts back to the actual upstream
- auth\_request\_set \$authentik\_username \$upstream\_http\_x\_authentik\_username;
- auth\_request\_set \$authentik\_groups \$upstream\_http\_x\_authentik\_groups;
- auth\_request\_set \$authentik\_email \$upstream\_http\_x\_authentik\_email;
- auth\_request\_set \$authentik\_name \$upstream\_http\_x\_authentik\_name;
- auth\_request\_set \$authentik\_uid \$upstream\_http\_x\_authentik\_uid;
- proxy\_set\_header X-authentik-username \$authentik\_username;
- proxy\_set\_header X-authentik-groups \$authentik\_groups;
- proxy\_set\_header X-authentik-email \$authentik\_email;
- proxy\_set\_header X-authentik-name \$authentik\_name;
- proxy\_set\_header X-authentik-uid \$authentik\_uid;
- }
- # all requests to /outpost.goauthentik.io must be accessible without authentication
- location /outpost.goauthentik.io {
- proxy\_pass http://0.0.0.0:3001/outpost.goauthentik.io;
- # ensure the host of this vserver matches your external URL you've configured
- # in authentik
- proxy\_set\_header Host \$host;
- proxy\_set\_header X-Original-URL \$scheme://\$http\_host\$request\_uri;
- add\_header Set-Cookie \$auth\_cookie;
- auth\_request\_set \$auth\_cookie \$upstream\_http\_set\_cookie;
- proxy\_pass\_request\_body off;
- proxy\_set\_header Content-Length "";
- }
- # Special location for when the /auth endpoint returns a 401,
- # redirect to the /start URL which initiates SSO
- location @goauthentik\_proxy\_signin {
- internal;
- add\_header Set-Cookie \$auth\_cookie;
- return 302 /outpost.goauthentik.io/start?rd=\$request\_uri;
- # For domain level, use the below error\_page to redirect to your authentik server with the full redirect path
- # return 302 https://authentik.company/outpost.goauthentik.io/start?rd=\$scheme://\$http\_host\$request\_uri;

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## A Anhang

---

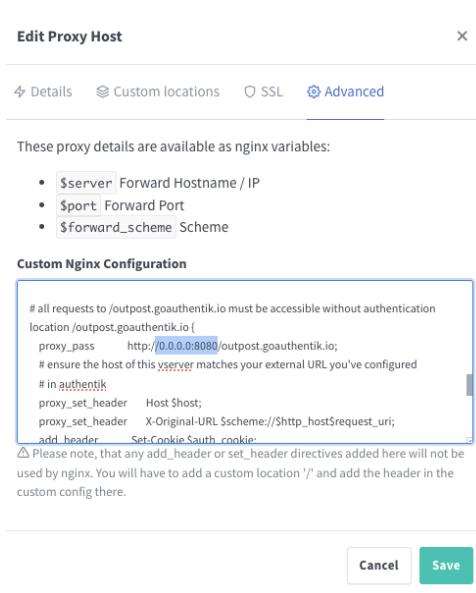


Abbildung 6: Proxy Host Konfiguration - Einfügen des Code-Snippets in den Bereich **Advanced** und erfolgt das Ändern der IP-Adresse mit dem zugehörigen Port

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

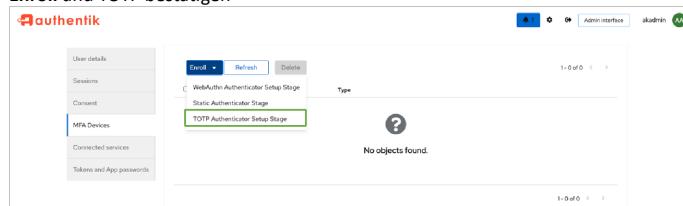
## A Anhang

### A.12 TOTP-Einrichtung

1. Login bei Authenthik

2. über Einstellungen, MFA-Devices auswählen

3. Enroll und TOTP bestätigen



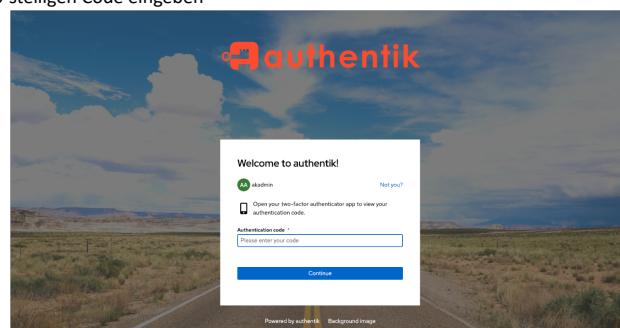
4. Logout bei Authenthik. Erneut Login bei Authenthik. QR-Code mit Microsoft Azure scannen

5. Erneut Login bei Authenthik

6. QR-Code mit Microsoft Azure scannen



7. 6-stelliger Code eingeben



8. Eingeloggt



# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## A Anhang

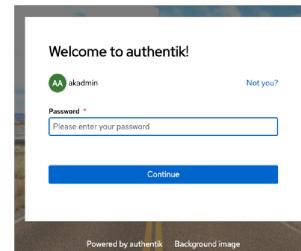
### A.13 Benutzerdokumentation

#### AUTHENTIK

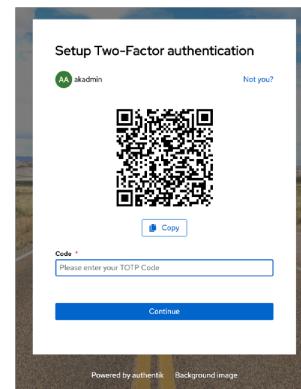
##### Was ist Authenik?

Authenik ist ein Open-Source-Identity-Provider mit dem Schwerpunkt auf Flexibilität und Vielseitigkeit. Es ist möglich Authenik in einer bestehenden Umgebung zu verwenden, um Unterstützung für neue Protokolle, Anmeldung/Wiederherstellung/etc. hinzuzufügen.

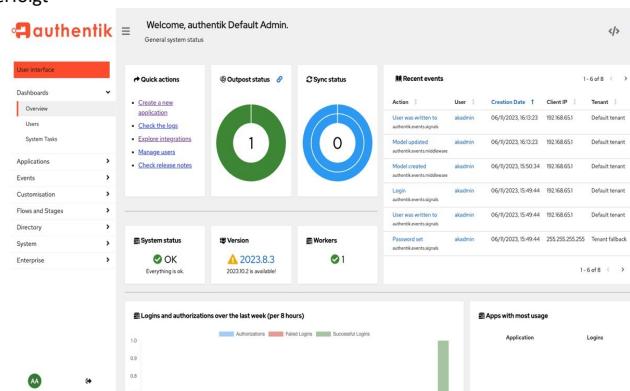
1. User erhalten Zugangsdaten für Authenik
2. User melden sich mit den Zugangsdaten für Authenik an (siehe Bild rechts)



3. Nach der ersten Anmeldung, werden die User durch einen QR-Code aufgefordert, den Microsoft Authenticator zu nutzen
4. Einen Account im Microsoft Authenticator hinzufügen und QR-Code scannen (rechts ein Bild des QR-Codes)



5. Dashboard, was erscheint, wenn eine direkte Anmeldung bei Authenik und nicht bei anderen Services erfolgt



## IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

A Anhang

### A.14 Testprotokoll

**Deloitte.**

---

**TEST-PROTOKOLL**

---

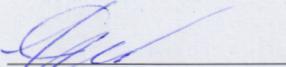
Von: Melissa Futtig

Datum: 08.11.2023

**Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur**

Testbeschreibung	Ergebnis
Problemlose Registrierung und einfacher Login	erfolgreich
Login als Admin und (einfacher) Benutzer	erfolgreich
Kompatibel mit einer Authenticator-Software	erfolgreich
Übersichtliches, englisches Willkommens-Display	erfolgreich
vor jeden konfigurierten Dienst schalten und nach Eingabe der Nutzerdaten freigeben	erfolgreich
Skalierbarkeit der Dienste	erfolgreich
Zugriff von Dritten verweigern	erfolgreich

Alle Anforderungen sind erfüllt.



Edgar Johann Kapler

---

Deloitte Wirtschaftsprüfungsgesellschaft GmbH  
Dittrichring 22  
04109 Leipzig

Tel +49 89 29036 – 0  
Fax +49 89 29036 – 8108  
E-Mail: [kontakt@deloitte.de](mailto:kontakt@deloitte.de)

## IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

A Anhang

### A.15 Übernahmeprotokoll

**Deloitte.**

---

**ÜBERNAHME-PROTOKOLL**

---

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

Testbeschreibung	Ergebnis
Problemlose Registrierung und einfacher Login	erfolgreich
Login als Admin und (einfacher) Benutzer	erfolgreich
Kompatibel mit einer Authenticator-Software	erfolgreich
Übersichtliches, englisches Willkommens-Display	erfolgreich
vor jeden konfigurierten Dienst schalten und nach Eingabe der Nutzerdaten freigeben	erfolgreich
Skalierbarkeit der Dienste	erfolgreich
Zugriff von Dritten verweigern	erfolgreich

Alle Anforderungen sind erfüllt.



Edgar Johann Kapler

Leipzig, 08.11.2023

---

Deloitte Wirtschaftsprüfungsgesellschaft GmbH  
Dittrichring 22  
04109 Leipzig

Tel +49 89 29036 – 0  
Fax +49 89 29036 – 8108  
E-Mail: [kontakt@deloitte.de](mailto:kontakt@deloitte.de)

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## *Abbildungsverzeichnis*

---

### **Abbildungsverzeichnis**

1	Use Case-Diagramm . . . . .	22
2	Sequenzdiagramm . . . . .	23
3	Cloud-Infrastruktur . . . . .	24
4	Docker Pull . . . . .	27
5	Docker Compose Up . . . . .	27
6	Proxy Host Konfiguration - Einfügen des Code-Snippets in den Bereich <b>Advanced</b> und erfolgt das Ändern der IP-Adresse mit dem zugehörigen Port . . . . .	33

# **IMPLEMENTIERUNG VON MFA**

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

*Tabellenverzeichnis*

---

## **Tabellenverzeichnis**

1	Zeitplanung . . . . .	5
2	Entscheidungsmatrix . . . . .	6
3	Personalplanung . . . . .	7
4	Kostenaufstellung . . . . .	8
5	Nutzwertanalyse zur MFA-Lösung . . . . .	12
6	Soll-/Ist-Vergleich . . . . .	17

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

## *Literaturverzeichnis*

---

### **Literaturverzeichnis**

#### **Authentik 2023**

AUTHENTIK, goauthentik: *Authentik*. <https://goauthentik.io/>. Version: 2023

#### **Composerize 2023**

COMPOSERIZE, composerize: *Composerize*. <https://www.composerize.com/>. Version: 2023

#### **Deloitte 2023**

DELOITTE, Deloitte: *Deloitte*. <https://www2.deloitte.com/de/de/pages/about-deloitte/articles/zahlen-fakten-de.html>. Version: 2023

#### **OVHCloud 2023**

OVHCLOUD, OVHCloud: *OVHCloud*. <https://www.ovhcloud.com/de/>. Version: 2023

#### **Pay-As-You-Go 2023**

PAY-AS-YOU-GO, Wikipedia: *Pay-As- You-Go*. <https://de.wikipedia.org/wiki/Pay-As-You-Go>. Version: 2023

#### **PDCA-Zyklus 2023**

PDCA-ZYKLUS, der-prozessmanager: *PDCA-Zyklus*. <https://der-prozessmanager.de/aktuuell/wissensdatenbank/pdca-zyklus>. Version: 2023

#### **BlackBox und WhiteBox 2023**

WHITEBOX, dev-insider BlackBox u.: *BlackBox und WhiteBox*. <https://www.dev-insider.de/der-unterschied-zwischen-black-box-und-white-box-test-a-1110525/#:~:text=Black%2DBox%2D%20und%20Glass%2D,k%C3%B6nnen%20sich%20im%20Gegenteil%20erg%C3%A4nzen.&text=White%20Box%20Testing%20und%20Black,der%20zu%20testenden%20Software%20verf%C3%BCgen>. Version: 2023

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

*Eidesstattliche Erklärung*

## Eidesstattliche Erklärung

 Industrie- und Handelskammer zu Leipzig

Geschäftsfeld Aus- und Weiterbildung

**Erklärung des Prüfungsteilnehmers / der Prüfungsteilnehmerin**

Ich versichere durch meine Unterschrift, dass ich das Projekt und die dazugehörige Dokumentation selbstständig und ohne fremde Hilfe angefertigt und alle Stellen, die ich wörtlich oder annähernd wörtlich aus Veröffentlichungen entnommen habe, als solche kenntlich gemacht habe. Die Arbeit hat in dieser Form keiner anderen Prüfungsinstanz vorgelegen.

Leipzig, 08.11.2023

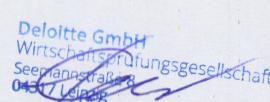
Ort, Datum



Unterschrift des Prüfungsteilnehmers

**Erklärung des Ausbildungsbetriebes / Praktikumsbetriebes**

Wir versichern, dass das Projekt wie in der Dokumentation dargestellt, in unserem Unternehmen realisiert worden ist.

  
Leipzig, 08.11.'23

Ort, Datum

Stempel und Unterschrift des Ausbildungsbetriebes

Geschäftsfeld Aus- und Weiterbildung  
Formular 04.09.26 Erklärung Prüfungsteilnehmer | Aktualisierung: 10.03.2014

Seite 1

# IMPLEMENTIERUNG VON MFA

Implementierung von Multi-Faktor-Authentifizierung (MFA) zur Erhöhung der Sicherheit bei der Zugriffskontrolle von verschiedenen Services in einer Cloud-Infrastruktur

*Nachweis zur Durchführung der betrieblichen Projektarbeit*

## Nachweis zur Durchführung der betrieblichen Projektarbeit

 Industrie- und Handelskammer zu Leipzig		
Geschäftsfeld Aus- und Weiterbildung		
<b>IT-Berufe – Nachweis über die Durchführung der betrieblichen Projektarbeit</b>		
Abschlussprüfung IT-Berufe		
Name, Vorname:  Futtig, Melissa	Berufsbezeichnung/Fachrichtung:  Fachinformatikerin für Systemintegration	
Prüflings-Nr.:  52065	Maximaler Zeitaufwand:  40 Stunden	
Datum	Anzahl der Stunden	ausgeführte Tätigkeiten
01.11.2023	8 Stunden	Planungsphase, Problemstellung, Ist- /Soll-Analyse
02.11.2023	8 Stunden	Projektdurchführung
03.11.2023	8 Stunden	Projektdurchführung
06.11.2023	4 Stunden	Testen
07.11.2023	4 Stunden	Übergabe in die Produktivumgebung
Anfertigung der Dokumentation:		
Datum	Anzahl der Stunden	
08.11.2023	8 Stunden	Projektdokumentation
Gesamt:	40 Stunden	
Ich versichere, dass ich die Projektarbeit einschließlich Dokumentation ohne fremde Hilfe und nur mit den angegebenen Hilfsmitteln erstellt habe. Das Projekt hat stattgefunden.		
Leipzig, 08.11.2023		
Ort, Datum	Unterschrift Prüfling	Unterschrift Betreuer
Geschäftsfeld Aus- und Weiterbildung Formular 4.6.1 IT-Berufe – Nachweis über die Durchführung der betrieblichen Projektarbeit   Aktualisierung: 01.10.2014		
		Seite 1