

## Über diese Vorlage

Diese L<sup>A</sup>T<sub>E</sub>X-Vorlage wurde von Stefan Macke<sup>1</sup> als Grundlage für die Projektdokumentationen der Auszubildenden zum Fachinformatiker mit Fachrichtung Anwendungsentwicklung bei der ALTE OLDENBURGER Krankenversicherung entwickelt. Nichtsdestotrotz dürfte sie ebenso für die anderen IT-Berufe<sup>2</sup> geeignet sein, da diese anhand der gleichen Verordnung bewertet werden.

Diese Vorlage enthält bereits eine Vorstrukturierung der möglichen Inhalte einer tatsächlichen Projektdokumentation, die auf Basis der Erfahrungen im Rahmen der Prüfertätigkeit des Autors erstellt und unter Zuhilfenahme von ROHRER UND SEDLACEK [2011] abgerundet wurden.

Sämtliche verwendeten Abbildungen, Tabellen und Listings stammen von GRASHORN [2010].

Download-Link für diese Vorlage: <http://fiaa.link/LaTeXVorlageFIAE>

Auch verfügbar auf GitHub: <https://github.com/StefanMacke/latex-vorlage-fiaa>

## Lizenz



Dieses Werk steht unter einer Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz.<sup>3</sup>



**Namensnennung** Sie müssen den Namen des Autors/Rechteinhabers in der von ihm festgelegten Weise nennen.<sup>4</sup>

**Weitergabe unter gleichen Bedingungen** Wenn Sie das lizenzierte Werk bzw. den lizenzierten Inhalt bearbeiten oder in anderer Weise erkennbar als Grundlage für eigenes Schaffen verwenden, dürfen Sie die daraufhin neu entstandenen Werke bzw. Inhalte nur unter Verwendung von Lizenzbedingungen weitergeben, die mit denen dieses Lizenzvertrages identisch oder vergleichbar sind.

---

<sup>1</sup>Blog des Autors: <http://fachinformatiker-anwendungsentwicklung.net>, Twitter: @StefanMacke

<sup>2</sup>z. B. IT-Kaufleute, Fachinformatiker mit Fachrichtung Systemintegration usw.

<sup>3</sup><http://creativecommons.org/licenses/by-sa/4.0/>

<sup>4</sup>Die Namensnennung im L<sup>A</sup>T<sub>E</sub>X-Quelltext mit Link auf <http://fiaa.link/LaTeXVorlageFIAE> reicht hierfür aus.

## Inhalt der Projektdokumentation

Grundsätzlich definiert die [REGIERUNG DER BUNDESREPUBLIK DEUTSCHLAND](#) [1997, S. 1746]<sup>5</sup> das Ziel der Projektdokumentation wie folgt:

„Durch die Projektarbeit und deren Dokumentation soll der Prüfling belegen, daß er Arbeitsabläufe und Teilaufgaben zielorientiert unter Beachtung wirtschaftlicher, technischer, organisatorischer und zeitlicher Vorgaben selbständig planen und kundengerecht umsetzen sowie Dokumentationen kundengerecht anfertigen, zusammenstellen und modifizieren kann.“

Und das [BUNDESMINISTERIUM FÜR BILDUNG UND FORSCHUNG](#) [2000, S. 36] ergänzt:

„Die Ausführung der Projektarbeit wird mit praxisbezogenen Unterlagen dokumentiert. Der Prüfungsausschuss bewertet die Projektarbeit anhand der Dokumentation. Dabei wird nicht das Ergebnis – z.B. ein lauffähiges Programm – herangezogen, sondern der Arbeitsprozess. Die Dokumentation ist keine wissenschaftliche Abhandlung, sondern eine handlungsorientierte Darstellung des Projektablaufs mit praxisbezogenen, d.h. betriebüblichen Unterlagen. Sie soll einen Umfang von maximal 10 bis 15 DIN A 4-Seiten nicht überschreiten. Soweit erforderlich können in einem Anhang z. B. den Zusammenhang erläuternde Darstellungen beigelegt werden.“

Außerdem werden dort die grundlegenden Inhalte der Projektdokumentation aufgelistet:

- Name und Ausbildungsberuf des Prüfungsteilnehmers
- Angabe des Ausbildungsbetriebes
- Thema der Projektarbeit
- Falls erforderlich, Beschreibung/Konkretisierung des Auftrages
- Umfassende Beschreibung der Prozessschritte und der erzielten Ergebnisse
- Gegebenenfalls Veränderungen zum Projektantrag mit Begründung
- Wenn für das Projekt erforderlich, ein Anhang mit praxisbezogenen Unterlagen und Dokumenten. Dieser Anhang sollte nicht aufgebläht werden. Die angehängten Dokumente und Unterlagen sind auf das absolute Minimum zu beschränken.

In den folgenden Kapiteln werden diese geforderten Inhalte und sinnvolle Ergänzungen nun meist stichwortartig und ggfs. mit Beispielen beschrieben. Nicht alle Kapitel müssen in jeder Dokumentation vorhanden sein. Handelt es sich bspw. um ein in sich geschlossenes Projekt, kann das Kapitel ??: ?? entfallen; arbeitet die Anwendung nur mit XML-Dateien, kann und muss keine Datenbank beschrieben werden usw.

---

<sup>5</sup>Dieses Dokument sowie alle weiteren hier genannten können unter <http://fiae.link/LaTeXVorlageFIAEQuellen> heruntergeladen werden.

## Formale Vorgaben

Die formalen Vorgaben zum Umfang und zur Gestaltung der Projektdokumentation können je nach IHK recht unterschiedlich sein. Normalerweise sollte die zuständige IHK einen Leitfaden bereitstellen, in dem alle Formalien nachgelesen werden können, wie z. B. bei der [IHK OLDENBURG \[2006\]](#).

Als Richtwert verwende ich 15 Seiten für den reinen Inhalt. Also in dieser Vorlage alle Seiten, die arabisch nummeriert sind (ohne das Literaturverzeichnis und die eidesstattliche Erklärung). Große Abbildungen, Quelltexte, Tabellen usw. gehören in den Anhang, der 25 Seiten nicht überschreiten sollte.

Typographische Konventionen, Seitenränder usw. können in der Datei `Seitenstil.tex` beliebig angepasst werden.

## Bewertungskriterien

Die Bewertungskriterien für die Benotung der Projektdokumentation sind recht einheitlich und können leicht in Erfahrung gebracht werden, z. B. bei der [IHK DARMSTADT \[2011\]](#). Grundsätzlich sollte die Projektdokumentation nach der Fertigstellung noch einmal im Hinblick auf diese Kriterien durchgeschaut werden.

## Prüfungsteil A

Prüfling (private Anschrift):	Ausbildungsbetrieb:
-------------------------------	---------------------

### Bestätigung über durchgeführte Projektarbeit

diese Bestätigung ist mit der Projektdokumentation einzureichen

Ausbildungsberuf (bitte unbedingt angeben):
---

Projektbezeichnung:
---------------------

Projektbeginn: _____	Projektfertigstellung: _____	Zeitaufwand in Std.: _____
----------------------	------------------------------	----------------------------

### Bestätigung der Ausbildungsfirma:

Wir bestätigen, dass der/die Auszubildende das oben bezeichnete Projekt einschließlich der Dokumentation im Zeitraum

vom: \_\_\_\_\_ bis: \_\_\_\_\_ selbständig ausgeführt hat.

Projektverantwortliche(r) in der Firma:

Vorname	Name	Telefon	Unterschrift
---------	------	---------	--------------

Ausbildungsverantwortliche(r) in der Firma:

Vorname	Name	Telefon	Unterschrift
---------	------	---------	--------------

### Eidesstattliche Erklärung:

Ich versichere, dass ich das Projekt und die dazugehörige Dokumentation selbständig erstellt habe.

Ort und Datum: \_\_\_\_\_ Unterschrift des Prüflings: \_\_\_\_\_



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 10.11.2023

**Prüfungsbewerber:**

Melissa Futtig  
Stephaniplatz 3  
04317 Leipzig

# **Deloitte.**

**Ausbildungsbetrieb:**

DELOITTE Wirtschaftsprüfungsgesellschaft GmbH

---

Dittrichring 22  
04109 Leipzig

**Inhaltsverzeichnis**

<b>Abbildungsverzeichnis</b>	<b>III</b>
<b>Tabellenverzeichnis</b>	<b>IV</b>
<b>Listings</b>	<b>V</b>
<b>Abkürzungsverzeichnis</b>	<b>VI</b>
<b>1 Einleitung</b>	<b>1</b>
1.1 Projektumfeld . . . . .	1
1.2 Projektziel . . . . .	1
1.3 Projektbegründung . . . . .	1
1.4 Projektschnittstellen . . . . .	2
1.4.1 Technisch . . . . .	2
1.4.2 Organisatorisch . . . . .	2
1.4.3 Personell . . . . .	3
<b>2 Projektplanung</b>	<b>3</b>
2.1 Projektphasen . . . . .	3
2.2 Abweichungen vom Projektantrag . . . . .	4
2.3 Ressourcenplanung . . . . .	4
2.3.1 Sachmittelplanung . . . . .	4
2.3.2 Personalplanung . . . . .	5
2.4 Entwicklungsprozess . . . . .	5
<b>3 Analysephase</b>	<b>5</b>
3.1 Ist-Analyse . . . . .	5
3.2 Soll-Analyse . . . . .	6
3.3 Wirtschaftlichkeitsanalyse . . . . .	6
3.3.1 „Make or Buy“-Entscheidung . . . . .	6
3.3.2 Projektkosten . . . . .	6
3.3.3 Amortisationsdauer . . . . .	7
3.4 Nicht-monetärer Nutzen . . . . .	8
3.5 Anwendungsfälle . . . . .	8
<b>4 Entwurfsphase</b>	<b>8</b>
4.1 Zielplattform . . . . .	8
4.2 Authentifizierungs-Tool . . . . .	9
4.3 Geschäftslogik . . . . .	9
4.4 Maßnahmen zur Qualitätssicherung . . . . .	10
4.5 Pflichtenheft/Datenverarbeitungskonzept . . . . .	10

*Inhaltsverzeichnis*


---

<b>5</b>	<b> Projektdurchführung</b>	<b>10</b>
5.1	Vorbereitung der Entwicklungsumgebung . . . . .	11
5.2	Auswahl einer MFA-Lösung . . . . .	11
5.2.1	Erstellung der docker-compose.yml, .env . . . . .	11
5.3	Installation und Konfiguration von Authentik . . . . .	11
5.4	Integration mit Cloud-Diensten . . . . .	11
5.5	Konfiguration des zweiten Faktors . . . . .	11
<b>6</b>	<b> Testphase</b>	<b>11</b>
6.1	Überwachung der Laufzeit der Services . . . . .	11
6.2	Zugriffstests . . . . .	11
<b>7</b>	<b> Dokumentation</b>	<b>11</b>
7.1	Entwicklerdokumentation . . . . .	12
<b>8</b>	<b> Fazit</b>	<b>12</b>
8.1	Soll-/Ist-Vergleich . . . . .	12
8.2	Lessons Learned . . . . .	12
8.3	Ausblick . . . . .	12
	<b>Literaturverzeichnis</b>	<b>13</b>
	<b>Eidesstattliche Erklärung</b>	<b>14</b>
<b>A</b>	<b> Anhang</b>	<b>ii</b>
A.1	Gantt . . . . .	ii
A.2	Detaillierte Zeitplanung . . . . .	iii
A.3	Use Case-Diagramm . . . . .	iii



**Abbildungsverzeichnis**

1	Use Case-Diagramm . . . . .	iv
---	-----------------------------	----

**Tabellenverzeichnis**

1	Zeitplanung . . . . .	4
2	Personalplanung . . . . .	5
3	Kostenaufstellung . . . . .	7
4	Entscheidungsmatrix . . . . .	9
5	Soll-/Ist-Vergleich . . . . .	12

## Listings

## **Abkürzungsverzeichnis**

<b>API</b>	Application Programming Interface
<b>EPK</b>	Ereignisgesteuerte Prozesskette
<b>XML</b>	Extensible Markup Language

## 1 Einleitung

### 1.1 Projektumfeld

Die Deloitte Wirtschaftsprüfungsgesellschaft GmbH ist ein internationales Unternehmen für Wirtschaftsprüfung, Steuer-, Unternehmens-, Risiko- und Finanzberatung. Die Deloitte hat Niederlassungen in vielen Ländern, darunter auch Deutschland. Mit Vertreter: innen in über 150 Ländern weltweit und 415.000 Mitarbeiter: innen bietet das Unternehmen eine breite Palette von Dienstleistungen für Unternehmen und Organisationen in verschiedenen Branchen. Im B&TCL, auch dem Business & Technology Center Leipzig, erbringt die Deloitte GmbH mit ihren 100 Mitarbeiter: innen 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 ist ein Tochterprojekt eines größeren und beinhaltet die Implementierung eines Teilfeatures, was zur Verbesserung des Gesamtprojektes führt. In diesem arbeiten interne Mitarbeiter: innen aktiv mit, um die Entwicklung des Projektes voranzutreiben. Dabei stellen diese die Zielgruppe dar.

### 1.2 Projektziel

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

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 Password-Leaks und Phishing vermieden werden können. Um das Ziel zu erreichen wird Authentik für die Implementierung von MFA auf verschiedene Services in der Cloud-Infrastruktur eingeführt. Dabei ist Authentik ein Open-Source-Identitätsanbieter (Identity Provider), der den Zugriff auf verschiedene Dienste und Ressourcen in der Cloud-Infrastruktur verwalten und sichern soll und legt den Fokus auf die Flexibilität und Vielseitigkeit.

### 1.3 Projektbegründung

Die Implementierung der MFA steigert die Sicherheit und gewährleistet, dass der Zugang zu Diensten und Daten in der Cloud-Infrastruktur nicht allein durch den Diebstahl eines Passworts gefährdet ist. Benutzer müssen zusätzlich zur Eingabe des Nutzernamens und Passworts einen weiteren Authentifizierungsfaktor, wie zum Beispiel ein Einmalpasswort, bereitstellen, was die Sicherheit erheblich erhöht. Dabei werden nicht nur firmeninterne und kundenbezogene Daten geschützt, sondern auch die Kundenzufriedenheit und das Vertrauen gegenüber der zukünftigen Kunden erhöht. Dies hat hohe Priorität und verhindert unbefugten Zugriff auf sensible Informationen.

## 1.4 Projektschnittstellen

### 1.4.1 Technisch

Die in Kapitel 1.2 besagte Cloud-Infrastruktur wird in vier Hauptbereiche unterteilt, sodass in jedem dieser Bereiche verschiedene Services bzw. Dienste zur Verfügung werden.

#### *Compliance and Security Stack*

Dieser Bereich umfasst den Einsatz von Docker-Containern für Dienste, 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. Der Guacamole Server dient als Proxy-Server und ermöglicht den Zugriff auf interne Dienste, die normalerweise nicht über eine Web-Schnittstelle erreichbar sind. Das Open-Source-Sicherheitstesttool Infection Monkey überprüft die Sicherheit der Infrastruktur. Mit dem Identity Provider Authentik, 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.

#### *Monitoring*

Im Überwachungsbereich werden alle vorhandenen Dienste mittels Docker-Containern der Cloud-Infrastruktur auditiert und beinhaltet dieser die Open-Source-Software Grafana zur Visualisierung und Überwachung von Leistungsdaten, sowie Uptime Kuma als Webserver für Statusseiten und Healthchecks, um die Verfügbarkeit der Dienste zu kontrollieren.

#### *DevOps*

Der Fokus diesen Bereiches liegt bei den Anwendungen in der Entwicklung und Bereitstellung und enthält die Kollaborationsplattform GitLab, um Projekte zu verwalten. Dabei werden diese Dienste mittels Docker-Containern hochgefahren. 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 Beispiele SSH-Schlüssel und Passwörter zu verwalten.

#### *E-Mail-Kommunikation*

In diesem Bereich werden Docker-Container eingesetzt, der den Mail-Server Mailcow hochfährt, um E-Mails zu senden und zu empfangen, SOGO als Groupware-Lösung und ermöglicht dadurch eine effiziente E-Mail-Kommunikation und Zusammenarbeit innerhalb und außerhalb der Organisation.

### 1.4.2 Organisatorisch

Nach der Implementierung Authentiks in der Cloud-Umgebung, erfolgen erste Tests und Validierungen in den erstellten Docker-Containern via 'docker-compose.yml-Dateien', um sicherzustellen, dass die MFA ordnungsgemäß funktioniert und den Sicherheitsanforderungen entspricht. Im Anschluss erfolgen Schulungen der Benutzer, in dem Fall das Entwicklerteam, zur genauen Verwendung von Authentik

## 2 Projektplanung

---

mit MFA. Nach den Tests und der Schulungen wird die Authentik-MFA-Implementierung in der Cloud-Umgebung bereitgestellt.

### 1.4.3 Personell

Das Projektteam besteht aus folgenden Personen:

- Projektauftraggeber/ Director: Herr Dr. Volker Stroetmann
- Projektleiter/ Manager/ Projektentwickler: Herr Edgar Johann Kapler
- Projektentwickler/ Auszubildender: Herr Dmytro Datsiuk
- Projektentwickler/ dualer Student: Herr Neo-Pascal Loest
- Projektentwicklerin/ duale Studentin: Frau Martyna Mol
- Projektentwickler/ Auszubildender: Herr Angelo Juliano Vogt
- Projektentwicklerin/ Auszubildende: Frau Melissa Futtig

Der Projektauftraggeber und -leiter sind die Verantwortlichen für die Projektleitung und -finanzierung des Projektes. Sie genehmigen dieses und stellen die notwendigen Ressourcen zur Entwicklung bereit. Die Projektentwickler: innen sind die allgemeinen Benutzer und das Entwicklerteam. Sie sind für die Umsetzung und den reibungslosen Betrieb der Cloud-Infrastruktur verantwortlich und benötigen sichere Zugriffsmöglichkeiten zu den bereitgestellten Anwendungen.

## 2 Projektplanung

### 2.1 Projektphasen

Das Projekt findet in zwei Wochen mit vier Stunden Arbeitszeit pro Tag statt, sodass Pufferzeit und Krankheit eingerechnet werden können.

Die im Projektantrag festgelegten Projektphasen lassen sich chronologisch in die 5-stündige Planungsphase, die 16-stündige Implementierungsphase, die 6-stündige Testphase, die 4-stündige Phase einteilen, in der die Einführung und Übergabe erfolgt und die 7-stündige Dokumentation mit der 2-stündigen Pufferzeit im Anschluss. Dabei änderte sich die Zeit in der Implementierungsphase von 14 auf 16 Stunden, die Zeit in der Dokumentation von 6 auf 7 Stunden und die Pufferzeit von 2 Stunden, welche hinzugefügt wurde, um zeitliche Konflikte mit den anderen Phasen zu vermeiden.

Tabelle 1 zeigt ein Beispiel für eine grobe Zeitplanung.

Eine detailliertere Zeitplanung findet sich im Anhang A.2: Detaillierte Zeitplanung auf Seite iii.

## 2 Projektplanung

Projektphase	Geplante Zeit
Planungsphase	5 h
Implementierungsphase	16 h
Testphase	6 h
Einführung und Übergabe	4 h
Dokumentation	7 h
Pufferzeit	2 h
<b>Gesamt</b>	<b>40 h</b>

Tabelle 1: Zeitplanung

### 2.2 Abweichungen vom Projektantrag

Die im Projektantrag mit "in Auflage genehmigten" Inhalte, erfordern Änderungen in der Projektdokumentation.

Die ursprüngliche Zeitplanung von 35 Stunden streckt sich auf 40 Stunden.

Im Anschluss passieren Änderungen in der Zeitplanung, im Schritt der Planungsphase, in welcher der Punkt "Klärung der Projektziele" in den Start dieser Phase geschoben wird.

Des Weiteren erfolgt in der Zeitplanung, der Dokumentation, in welchem geplant keine Entwicklerdokumentation stattfindet, sondern gewünscht eine Benutzerdokumentation.

Die technische Umsetzung von Sitecars sollte sich in der Implementierungsphase nach der Auswahl einer MFA-Lösung ereignen, was bedingt der Nutzwertanalyse auf der Seite 9 im Kapitel 4: Authentifizierungstool auf Authentik änderte.

### 2.3 Ressourcenplanung

#### 2.3.1 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
- IDE - Visual Studio Code 1.83.1 (user setup)
- Docker-Containerisierung auf der OVHCloud-Infrastruktur in einer Linux-Umgebung
- OVHCloud-Instanz - firewall\_instance\_dev (flavor name: b2-7)
- OVHCloud-Instanz - tal\_cloud\_infra (flavor name: r2-60)
- OVHCloud-Instanz - rev\_prox-dev (flavor name: b2-15)



### 3 Analysephase

#### 2.3.2 Personalplanung

Tabelle 2 zeigt die Personalplanung des Projektes.

Name	Rolle/ Berufsbezeichnung	Zeitaufwand
Dr. Volker Stroetmann	Director	0 h
Edgar Johann Kapler	Manager	1 h
Neo-Pascal Loest	dualer Student	0 h
Martyna Mol	duale Studentin	0 h
Birk Spinn	dualer Student	4 h
Dmytro Datsiuk	Auszubildender	0 h
Angelo Juliano Vogt	Auszubildender	0 h
Melissa Futtig	Auszubildende	42 h

Tabelle 2: Personalplanung

#### 2.4 Entwicklungsprozess

Das Projekt unterteilt sich in einem überschaubaren, zeitlich und inhaltlich begrenzten Entwicklungsprozess mit einzelnene begrenzten Phasen, die nach- und voneinander aufbauen. So wird eine Sicherstellung der Schritt für Schritt-Beendigung der jeweiligen Phasen und Übersicht gewährleistet. Bedingt dessen, dass in diesem Projekt wenig Projektteilnehmer: innen zur Verfügung stehen, kann auf die agile Methodik verzichtet werden.

## 3 Analysephase

### 3.1 Ist-Analyse

Das Projekt, operiert durch die Deloitte Wirtschaftsprüfungsgesellschaft GmbH, verwendet die Cloud-Infrastruktur von OVHCloud, um einen Business Hosting Service bereitzustellen. Dabei enthält diese Konfiguration der Cloud-Umgebung eine Firewall, welcher eine öffentliche IP-Adresse zugewiesen bekommen hat. Zusätzlich sollte erwähnt werden, dass dieses Netzwerk privat ist und andere Services und Instanzen enthält, welche von der Firewall geschützt werden. Um einen Zugriff auf die Instanzen zu ermöglichen, wird den Command-Line-Interface-Usern die Möglichkeit geboten, über die Kontrollinstanz "control\_node" die Instanzen hoch- und runterzufahren und die grundlegenden Einstellungen, wie zum Beispiel Portzuweisungen, vorzunehmen. Die Graphical-User-Interface-User haben des Weiteren die Chance die Services über den Nginx Proxy Manager zu erreichen, indem der Zugriff klassisch mittels einer einfachen Nutzer- und Passwordeingabe, ohne einer weiteren Schutzebene erfolgt.

## 3.2 Soll-Analyse

Das Soll des Projektes ist es die Dienste mittels Authentik durch die MFA zu schützen. Dabei wird vor jedem Service der Identity-Provider Authentik vorgeschaltet, sodass nicht nur MFA, sondern auch SSO passiert und die User automatisch authentifiziert werden und das Schutzziel Authentizität erfüllt wird.

Schlussfolgernd ist zu sagen, dass der Benutzer sich vor jeder Anmeldung bei einem Service sich erst bei Authentik anmeldet, um auf den gewünschten Dienst zugreifen zu können.

## 3.3 Wirtschaftlichkeitsanalyse

Durch die schon vorhandene Cloud-Infrastruktur 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 Speicher und mehr Rechenleistung benötigt, welche auf der vorhandenen Instanz zur Verfügung stehen und die beiden Faktoren das Arbeiten der Instanz nicht beeinträchtigen und resultierend daraus keine größere Instanz notwendig ist. Die wirklich zu entstehenden Kosten sind ausschließlich Personal- und Materialkosten, wobei letztere aus der Nutzung des Büromöbelars zusammengefasst wird.

Durch die Einführung von MFA durch Authentik 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. Des Weiteren erfolgen Kostenersparnisse in dem Punkt des Verhinderns der Passwort-Resets durch das Anfragen des administrativen Supports, bei welchem Zeit und daraus Kosten entstehen, die vermieden werden können. Durch die Implementierung kann den Nutzern ein sicherer und bequemerer Zugriff gewährleistet und die Kosten gesenkt werden.

### 3.3.1 „Make or Buy“-Entscheidung

In der Entscheidungsmatrix für die Zielplattform aus dem Kapitel 4.2: Authentifizierungs-Tool auf der Seite 9 sind einige alternative Produkte sichtbar, welche wie Authentik, implementiert werden müssen.

### 3.3.2 Projektkosten

Die Kosten für die Durchführung des Projekts setzen sich aus den Personal- und Ressourcenkosten zusammen.

## 3 Analysephase

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

$$1400 \text{ €/Monat} \cdot 12 \text{ Monate/Jahr} = 16800 \text{ €/Jahr} \quad (2)$$

$$\frac{16800 \text{ €/Jahr}}{1760 \text{ h/Jahr}} \approx 9,55 \text{ €/h} \quad (3)$$

Anhand der oben genannten Formel ergibt sich ein Stundenlohn von 9,55 €.

Die Durchführungszeit des Projekts beträgt 40 Stunden. Dabei sind mögliche 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.) oder das Möbelar, was pauschal mit 15,00 € kalkuliert werden kann. Das Brutto-Einkommen eines Auszubildenden im 3. Lehrjahr im Fachbereich Fachinformatik bei der Deloitte Wirtschaftsprüfungsgesellschaft GmbH beträgt 1400,00 € pro Monat. Für die weiteren Mitarbeiter werden pauschale Beträge zur Berechnung des Stundensatzes genutzt, aus den Gründen, dass die Deloitte Wirtschaftsprüfungsgesellschaft GmbH die Kosten pro Stunde nicht preisgeben möchte. Duale Studenten werden pauschal mit 15,00 €, während die Manager mit 50,00 € pro Stunde berechnet werden. Bei jeweils beiden addiert sich die Summe der Ressourcenkosten auf. Die Gesamtkosten, dargestellt in der Tabelle 3 betragen 1228,78 €.

Vorgang	Zeit	Kosten pro Stunde	Kosten
Arbeitskosten	41 h	9,55 € + 15,00 € = 24,55 €	1031,10 €
Unterstützungskosten (Manager)	1 h	50,00 € + 15,00 € = 65,00 €	65,00 €
Unterstützungskosten (dualer Student)	4 h	15,00 € + 15,00 € = 30,00 €	120,00 €
Abnahmetest	1 h	25,00 € + 15,00 € = 40,00 €	80 €
OVHCloud-Kosten	40 h	0,317 € + 0,00 € = 0,317 €	12,68 €
			<b>1.228,78 €</b>

Tabelle 3: Kostenaufstellung

### 3.3.3 Amortisationsdauer

Die Amortisation beschleunigt sich durch die Verwendung von Docker, GitLab und Authentik, was die Einsparung von Lizenzkosten zur Folge hat. 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. Im Vergleich zu einigen kostenpflichtigen Virtualisierungslösungen, wie z. B. Microsoft Hyper-V, können also Lizenzkosten eingespart werden. Des Weiteren ermöglicht Docker eine Arbeitszeiterparnis durch die einfache Bereitstellung und Verwaltung von Diensten, was die Arbeitszeit für die Einrichtung und Wartung von Umgebungen verkürzt.

### 3.4 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 ??: ?? 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.

### 3.5 Anwendungsfälle

Ein Use Case-Diagramm zur Veranschaulichung des Prozesses der Cloud-Infrastruktur findet sich im Anhang A.3: Use Case-Diagramm auf Seite iii. 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 erfolgreicher 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 Server Core) und dem integrierten Außenposten (Embedded outpost) besteht. Einkommende Anfragen an den Server-Containern werden an den Authentik Server Core oder dem Embedded outpost 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 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.

## 4 Entwurfsphase

### 4.1 Zielplattform

Die zu resultierende Zielplattform definiert sich über die Benutzerfreundlichkeit, Sicherheit, Implementierung, Dokumentation und Skalierbarkeit und entscheidet sich durch die im Kapitel ??: ?? dargestellte Nutzwertanalyse.

## 4.2 Authentifizierungs-Tool

Anhand der Entscheidungsmatrix in Tabelle 4 wurde Authentik ausgewählt.

Die in Kapitel 4.1: Zielplattform erwähnten Eigenschaften tragen zur Entscheidungsfindung bei, sodass sich anhand der gegebenen Entscheidungsmatrix Authentik herauskristallisierte.

Eigenschaft	Wertung	Authentik	Authelia	Sitecar	Micr. Az. AD
Benutzerfreundlichkeit	15	15	15	12	14
Sicherheit (OAuth, 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 4: Entscheidungsmatrix

Die Gewichtung hat einen Gesamtwert von 100 Wertungspunkten mit einem Maximalwert von 25 und Mindestwert von 15. Grund dafür sind die unterschiedlichen Eigenschaften, welche in der Entwicklung und bei der Auswahl der Authentifizierungsmethode jeweils verschiedene Rollen spielen und resultierend daraus variierend evaluiert werden. Nach der Zuordnung und Addierung der Punkte bei den drei Authentifizierungs-Tools, wird die Gesamtheit aller durch den Wert 100 dividiert und das Endergebnis ausgerechnet. Dabei hat die Einhaltung der Sicherheit Priorität und erhält den Maximalwert von 25 Punkten, bedingt dessen, dass Dritten der Zugriff auf die jeweiligen Dienste mit kunden- und firmeninternen Daten der Cloud-Infrastruktur verweigert werden sollte. Die Benutzerfreundlichkeit, Skalierbarkeit und Implementierung werden mit 20 Punkten bewertet, aufgrund der Tatsache, dass 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 Relevanz, weil die Möglichkeit besteht, Dienste hinzuzufügen oder rauszunehmen. Am wenigsten bedeutend ist die Dokumentation, welche gleichermaßen nicht zu unterschätzen ist, da eine gut geschriebene Dokumentation des Herstellers die Entwicklung enorm beeinflusst und erleichtert.

## 4.3 Geschäftslogik

- Modellierung und Beschreibung der wichtigsten (!) Bereiche der Geschäftslogik (z. B. mit Komponenten-, Klassen-, Sequenz-, Datenflussdiagramm, Programmablaufplan, Struktogramm, Ereignisgesteuerte Prozesskette (EPK)).
- Wie wird die erstellte Anwendung in den Arbeitsfluss des Unternehmens integriert?

#### 4.4 Maßnahmen zur Qualitätssicherung

- Welche Maßnahmen werden ergriffen, um die Qualität des Projektergebnisses (siehe Kapitel ??: ??) zu sichern (z. B. automatische Tests, Anwendertests)?
- Ggfs. Definition von Testfällen und deren Durchführung (durch Programme/Benutzer).

#### 4.5 Pflichtenheft/Datenverarbeitungskonzept

- Auszüge aus dem Pflichtenheft/Datenverarbeitungskonzept, wenn es im Rahmen des Projekts erstellt wurde.

**Beispiel** Ein Beispiel für das auf dem Lastenheft (siehe Kapitel ??: ??) aufbauende Pflichtenheft ist im Anhang ??: ?? auf Seite ?? zu finden.

### 5 Projektdurchführung

Hinweis: Wie in Kapitel 1: Einleitung zitiert, wird nicht ein lauffähiges Programm bewertet, sondern die Projektdurchführung. Dennoch würde ich immer Quelltextausschnitte zeigen, da sonst Zweifel an der tatsächlichen Leistung des Prüflings aufkommen können.

## 6 Testphase

---

### 5.1 Vorbereitung der Entwicklungsumgebung

### 5.2 Auswahl einer MFA-Lösung

#### 5.2.1 Erstellung der docker-compose.yml, .env

### 5.3 Installation und Konfiguration von Authentik

### 5.4 Integration mit Cloud-Diensten

### 5.5 Konfiguration des zweiten Faktors

## 6 Testphase

### 6.1 Überwachung der Laufzeit der Services

### 6.2 Zugriffstests

## 7 Dokumentation

- Wie wurde die Anwendung für die Benutzer/Administratoren/Entwickler dokumentiert (z. B. Benutzerhandbuch, API-Dokumentation)?
- Hinweis: Je nach Zielgruppe gelten bestimmte Anforderungen für die Dokumentation (z. B. keine IT-Fachbegriffe in einer Anwenderdokumentation verwenden, aber auf jeden Fall in einer Dokumentation für den IT-Bereich).

**Beispiel** Ein Ausschnitt aus der erstellten Benutzerdokumentation befindet sich im Anhang ??: ?? auf Seite ??. Die Entwicklerdokumentation wurde mittels PHPDoc<sup>6</sup> automatisch generiert. Ein beispielhafter Auszug aus der Dokumentation einer Klasse findet sich im Anhang ??: ?? auf Seite ??.

---

<sup>6</sup>Vgl. [PHPDOC.ORG](https://phpdoc.org) [2010]

## 7.1 Entwicklerdokumentation

# 8 Fazit

## 8.1 Soll-/Ist-Vergleich

- Wurde das Projektziel erreicht und wenn nein, warum nicht?
- Ist der Auftraggeber mit dem Projektergebnis zufrieden und wenn nein, warum nicht?
- Wurde die Projektplanung (Zeit, Kosten, Personal, Sachmittel) eingehalten oder haben sich Abweichungen ergeben und wenn ja, warum?
- Hinweis: Die Projektplanung muss nicht strikt eingehalten werden. Vielmehr sind Abweichungen sogar als normal anzusehen. Sie müssen nur vernünftig begründet werden (z. B. durch Änderungen an den Anforderungen, unter-/überschätzter Aufwand).

**Beispiel (verkürzt)** Wie in Tabelle 5 zu erkennen ist, konnte die Zeitplanung bis auf wenige Ausnahmen eingehalten werden.

Phase	Geplant	Tatsächlich	Differenz
Entwurfsphase	19 h	19 h	
Analysephase	9 h	10 h	+1 h
Implementierungsphase	29 h	28 h	-1 h
Abnahmetest der Fachabteilung	1 h	1 h	
Einführungsphase	1 h	1 h	
Erstellen der Dokumentation	9 h	11 h	+2 h
Pufferzeit	2 h	0 h	-2 h
<b>Gesamt</b>	<b>70 h</b>	<b>70 h</b>	

Tabelle 5: Soll-/Ist-Vergleich

## 8.2 Lessons Learned

- Was hat der Prüfling bei der Durchführung des Projekts gelernt (z. B. Zeitplanung, Vorteile der eingesetzten Frameworks, Änderungen der Anforderungen)?

## 8.3 Ausblick

- Wie wird sich das Projekt in Zukunft weiterentwickeln (z. B. geplante Erweiterungen)?



## Literaturverzeichnis

### Bundesministerium für Bildung und Forschung 2000

BUNDESMINISTERIUM FÜR BILDUNG UND FORSCHUNG: Umsetzungshilfen für die neue Prüfungsstruktur der IT-Berufe / Bundesministerium für Bildung und Forschung. Version: Juli 2000. <http://fiae.link/UmsetzungshilfenITBerufe>. Bonn, Juli 2000. – Abschlussbericht. – 476 S.

### Grashorn 2010

GRASHORN, Dirk: Entwicklung von NatInfo – Webbasiertes Tool zur Unterstützung der Entwickler / Alte Oldenburger Krankenversicherung AG. Vechta, April 2010. – Dokumentation zur Projektarbeit

### IHK Darmstadt 2011

IHK DARMSTADT: *Bewertungsmatrix für Fachinformatiker/innen Anwendungsentwicklung*. <http://fiae.link/BewertungsmatrixDokuDarmstadt>. Version: März 2011

### IHK Oldenburg 2006

IHK OLDENBURG: *Merkblatt zur Abschlussprüfung der IT-Berufe*. <http://fiae.link/MerkblattDokuOldenburg>. Version: Mai 2006

### phpdoc.org 2010

PHPDOC.ORG: *phpDocumentor-Website*. Version: 2010. <http://www.phpdoc.org/>, Abruf: 20.04.2010

### Regierung der Bundesrepublik Deutschland 1997

REGIERUNG DER BUNDESREPUBLIK DEUTSCHLAND: *Verordnung über die Berufsausbildung im Bereich der Informations- und Telekommunikationstechnik*. <http://fiae.link/VerordnungITBerufe>. Version: Juli 1997

### Rohrer und Sedlacek 2011

ROHRER, Anselm ; SEDLACEK, Ramona: *Cleverer Tipps für die Projektarbeit - IT-Berufe: Abschlussprüfung Teil A*. 5. Solingen : U-Form-Verlag, 2011 <http://fiae.link/ClevererTippsFuerDieProjektarbeit>. – ISBN 3882347538

## Eidesstattliche Erklärung

Ich, Melissa Futtig, versichere hiermit, dass ich meine **Dokumentation zur betrieblichen Projektarbeit** mit dem Thema

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

selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe, wobei ich alle wörtlichen und sinngemäßen Zitate als solche gekennzeichnet habe. Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch nicht veröffentlicht.

Leipzig, den 10.11.2023

---

MELISSA FUTTIG



A Anhang

A.1 Gantt

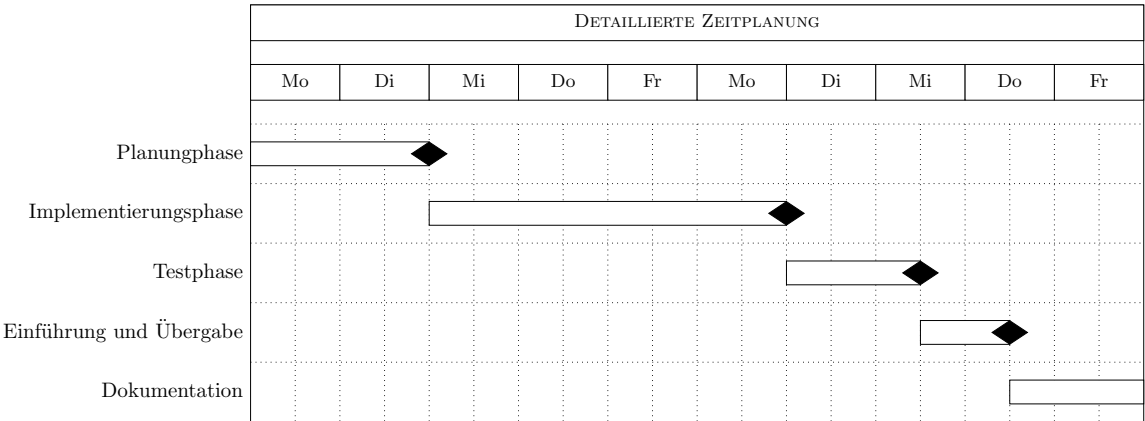


Figure 1: Gantt Chart

0.1 Gantt

## A.2 Detaillierte Zeitplanung

<b>1. Planungsphase</b>	<b>5 h</b>
1. Klärung der Projektziele	1 h
1.2. Erstellen einer Ist-Analysephase	1 h
1.3. Erstellen einer Soll-Analyse	1 h
1.4. Kostenplanung	0.5 h
1.5. Projektumfeldklärung	0.5 h
1.6. Kosten- und Nutzwertanalyse	0.5 h
1.7. Erstellung des Gantt-Diagramms	0.5 h
<b>2. Implementierungsphase</b>	<b>16 h</b>
2.1. Vorbereitung der Entwicklungsumgebung	1.5 h
2.2 Auswahl einer MFA-Lösung	0.5 h
2.3. Erstellung der docker-compose.yml- und .env-Dateien	1.5 h
2.4. Installation und Konfiguration von Authentik	5.5 h
2.5. Konfiguration der MFA	2.5 h
2.6. Integration mit Cloud-Diensten	4 h
2.7. Konfiguration des zweiten Faktors	1 h
<b>3. Testphase</b>	<b>6 h</b>
3.1. Überwachung der Laufzeit der Services	0.5 h
3.2. Überprüfung/ Beseitigung von Fehlern	4 h
3.3. Zugriffstest	1.5 h
<b>4. Einführung und Übergabe</b>	<b>4 h</b>
4.1. Ausführung und Ergebnisübergabe	3 h
4.2. Schulung der zu Beteiligten für die Nutzung	1 h
<b>5. Dokumentation</b>	<b>7 h</b>
5.1 Erstellung einer Projektdokumentation der Ergebnisse	6 h
5.3. Erstellung der Benutzerdokumentation	1 h
<b>6. Pufferzeit</b>	<b>2 h</b>
6.1. Puffer	2 h
<b>Gesamt</b>	<b>40 h</b>

## A.3 Use Case-Diagramm

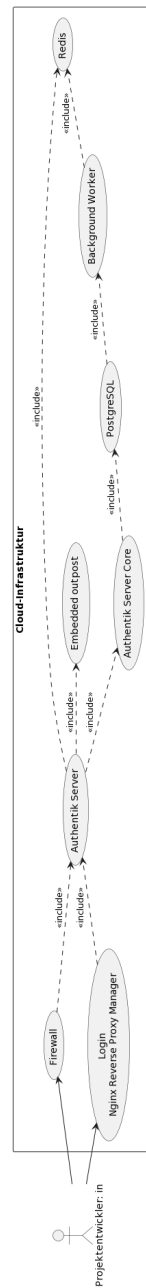


Abbildung 1: Use Case-Diagramm