TU WIEN Informatics

A Unified Multi-Factor Authentication Strategy: Enhancing Security in Academic Institutions with a Case Study of TU Wien

Challenges, Design Considerations, and Implementation Pathways

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Business Informatics

eingereicht von

Georg Natter, BSc.
Matrikelnummer 11708469

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: Ao.Univ.Prof. Ing. Mag. Dr. Horst Eidenberger

Wien, 16. März 2025

Georg Natter	Horst Eidenberger

Technische Universität Wien
A-1040 Wien ▪ Karlsplatz 13 ▪ Tel. +43-1-58801-0 ▪ www.tuwien.at

TU WIEN Informatics

A Unified Multi-Factor Authentication Strategy: Enhancing Security in Academic Institutions with a Case Study of TU Wien

Challenges, Design Considerations, and Implementation Pathways

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Business Informatics

by

Georg Natter, BSc.
Registration Number 11708469

to the Faculty of Informatics

at the TU Wien

Advisor: Ao.Univ.Prof. Ing. Mag. Dr. Horst Eidenberger

Vienna, March 16, 2025

Georg Natter

Horst Eidenberger

Technische Universität Wien
A-1040 Wien ▪ Karlsplatz 13 ▪ Tel. +43-1-58801-0 ▪ www.tuwien.at

Erklärung zur Verfassung der Arbeit

Georg Natter, BSc.

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.
Ich erkläre weiters, dass ich mich generativer KI-Tools lediglich als Hilfsmittel bedient habe und in der vorliegenden Arbeit mein gestalterischer Einfluss überwiegt. Im Anhang „Overview of Generative AI Tools Used“ habe ich alle generativen KI-Tools gelistet, die verwendet wurden, und angegeben, wo und wie sie verwendet wurden. Für Textpassagen, die ohne substantielle Änderungen übernommen wurden, habe ich jeweils die von mir formulierten Eingaben (Prompts) und die verwendete IT- Anwendung mit ihrem Produktnamen und Versionsnummer/Datum angegeben.

Wien, 16. März 2025

Georg Natter

Danksagung

Ich möchte meinem Betreuer, Ao.Univ.Prof. Ing. Mag. Dr. Horst Eidenberger, meinen aufrichtigen Dank für seine kontinuierliche Unterstützung, seine wertvolle fachliche Orientierungshilfe und sein außergewöhnlich schnelles Feedback während dieser Forschungsarbeit aussprechen. Außerdem danke ich allen Interviewteilnehmenden, die großzügig ihre Zeit und ihr Fachwissen geteilt haben.

Acknowledgements

I would like to express my sincere gratitude to my supervisor, Ao.Univ.Prof. Ing. Mag. Dr. Horst Eidenberger, for his continuous support, insightful guidance, and exceptionally prompt feedback throughout this research. I also extend my appreciation to all the interview participants who generously shared their time and expertise.

Kurzfassung

Die zunehmende Abhängigkeit von digitalen Diensten an akademischen Institutionen und die steigende Ausgereiftheit von Cyber-Bedrohungen erfordern sichere und skalierbare Identity & Access Management-Lösungen (IAM). Während Multi-Faktor-Authentifizierung (MFA) als effektive Sicherheitsmaßnahme weithin anerkannt ist, stellt ihre Implementierung im Hochschulbereich besondere Herausforderungen dar. Dazu gehören die Widerstände der Studierenden sowie technische Integrationsschwierigkeiten aufgrund fragmentierter Authentifizierungssysteme und veralteter Infrastruktur. Infolgedessen setzen viele Hochschulen, darunter auch die TU Wien, hauptsächlich auf Single-Faktor-Authentifizierung (SFA), um den Zugriff auf ihre Systeme zu sichern. Diese Abhängigkeit von SFA birgt erhebliche Sicherheitsrisiken, insbesondere da diese Systeme oft große Mengen sensibler Informationen über verschiedene Plattformen hinweg verarbeiten, auf die Studierende zugreifen können.

Diese Masterarbeit untersucht diese Herausforderungen und schlägt eine vereinheitlichende MFA-Strategie vor, um die Datensicherheit in akademischen Institutionen zu verbessern, wobei die TU Wien als Fallstudie dient. Um dieses Ziel zu erreichen, umfasst der methodische Ansatz drei Forschungsansätze. Erstens wurde eine systematische Literaturrecherche durchgeführt, um bestehende MFA-Lösungen, deren Akzeptanz in kommerziellen und akademischen Umgebungen sowie deren Einfluss auf Sicherheit und Nutzerverhalten zu analysieren. Zweitens wurden semi-strukturierte Interviews mit IT-Sicherheitsexpert:innen und weiteren Stakeholder:innen österreichischer Universitäten durchgeführt, um praktische Herausforderungen und Überlegungen zu identifizieren. Dabei wurden technische Einschränkungen, organisatorische Strategien und Akzeptanzfaktoren von MFA-Implementierungen untersucht. Drittens wurden die gesammelten Daten mittels Framework-Analyse in eine konzeptionelle Strategie überführt und ein Prototyp entwickelt.

Die vorgeschlagene Strategie für die Implementierung eines einheitlichen MFA-Systems in akademischen Institutionen eine schrittweise Einführung, flexible Authentifizierungsoptionen und nutzerzentrierte Adoptionsstrategien. Eine praktische Demonstration mit Keycloak unter Verwendung des entwickelten Prototyps validiert die vorgeschlagene Strategie, indem sie Einblicke in die simulierte Realisierbarkeit liefert. Die Ergebnisse zeigen, dass schrittweise implementierte MFA-Lösungen mit mehreren wählbaren Authentifizierungsmethoden die Sicherheit erhöhen und gleichzeitig die Benutzerfreund-

lichkeit verbessern. Darüber hinaus erfordert eine erfolgreiche Einführung von MFA einen zentralisierten IAM-Ansatz, der bestehende fragmentierte Authentifizierungsdienste konsolidiert. Open-Source-Lösungen wie Keycloak bieten eine praktikable Möglichkeit, MFA in komplexe IT-Infrastrukturen von Universitäten zu integrieren.

Abstract

An increasing reliance on digital services in academic institutions and the growing sophistication of cyber threats necessitate secure and scalable identity & access management (IAM) solutions. While multi-factor authentication (MFA) is widely recognized as an effective security measure, its implementation in higher education presents unique challenges. These include user resistance, and technical integration difficulties due to fragmented authentication systems and legacy infrastructure. As a result, many institutions of higher education, including TU Wien, predominantly use single-factor authentication (SFA) mechanisms to secure access to their systems. This reliance on SFA poses significant security challenges, especially as these systems often handle vast amounts of sensitive information across multiple platforms that students can access.

This thesis investigates these challenges and proposes a unified MFA strategy to enhance the security of data in academic institutions, with TU Wien serving as a case study. To achieve this, the methodological approach consists of three research methods. First, a systematic literature review (SLR) was applied to examine existing MFA solutions, their adoption in commercial and academic settings, and their impact on security and user behavior. Secondly, semi-structured interviews (SSIs) provided insights into practical challenges and considerations by engaging IT security experts and other stakeholders of Austrian universities. These interviews explored technical constraints, organizational strategies, and user acceptance factors in MFA deployments. Finally, by following the framework analysis research method, the collected data was transformed into a conceptual strategy and a prototype was developed.

The proposed strategy for implementing a unified MFA system in academic institutions emphasizes phased rollouts, flexible authentication options, and user-centric adoption strategies. A practical demonstration of Keycloak using the implemented prototype validates the proposed strategy by providing insights into simulated real-world feasibility. The findings indicate that phased MFA implementations with multiple MFA methods to chose from improve security while maintaining better usability. Furthermore, the successful deployment of MFA requires a centralized IAM approach that consolidates existing fragmented authentication services. Open-source solutions like Keycloak offer a viable approach to integrating MFA in complex university IT infrastructures.

Contents

CHAPTER 1

Introduction

1.1 Motivation

The rapid digitization of university operations and the increasing sophistication of cyber threats necessitate secure measures to protect data and maintain integrity within academic institutions. Many institutions of higher education, including TU Wien, predominantly use single-factor authentication (SFA) mechanisms to secure access to their systems. This reliance on SFA poses significant security challenges, especially as these systems often handle vast amounts of sensitive information across complex IT infrastructures with multiple platforms that students can access. [Lin22]

Single-factor authentication, typically involving a single credential such as a password, is inherently less secure than multi-factor authentication (MFA). It exposes institutions to increased risks of unauthorized access and potential data breaches due to the ease with which passwords can be compromised, e.g., through methods such as phishing and brute force attacks. The U.S. Department of Education has highlighted that hackers commonly exploit the existence of SFA in higher education institutions, emphasizing the critical need for enhanced identity management and MFA. [Zim18]

1.2 Problem Statement

Despite the availability of more secure authentication options, the adoption of two-factor authentication (2FA) and MFA remains low in many academic settings. For instance, at TU Wien, identities are managed through three sources that use different authentication mechanisms. Even though the main student platform provides optional two-factor authentication, this additional level of security is rarely used by students. This scenario further highlights the need for unified multi-factor authentication (MFA) solutions that integrate seamlessly with existing IT landscapes. Besides securing access more effectively,

it is imperative that solutions ensure or facilitate student acceptance for any potential additional factors of authentication.

This thesis aims to propose a unified multi-factor authentication strategy to enhance the security of data and access controls in academic institutions, with TU Wien serving as a case study within expert interviews. The system will have to cope with complex existing IT infrastructures, which includes multiple sources for accounts and identities. The research will compare different approaches to mitigate the risks associated with a reliance on single-factor authentication methods, striving for suitable MFA solutions. A practical prototype using Keycloak will be implemented to demonstrate the feasibility and potential integration scenarios. Besides improving security standards, it is crucial that the proposed solution is also feasible in terms of user acceptance. Interviews with IT security experts and other stakeholders will provide qualitative data to help properly formulate both system and user requirements. This thesis therefore also aims to present critical insights into user acceptance, evaluating various secure authentication approaches, from less obtrusive to highly stringent methods.

The work will address the following research questions:

1. What technical and user acceptance challenges must be considered when implementing a unified MFA system in an academic environment, and how do these challenges differ from those in other types of organizations?
2. How can MFA systems be tailored to meet the specific needs and constraints of higher-education environments while ensuring high user adoption?
3. What role can Keycloak[1], an open-source identity and access management solution, play in the architecture of a robust MFA system designed for educational environments?

1.3 Methodological Approach

This research employs a mixed-methods approach, combining a systematic literature review (SLR), semi-structured interviews (SSIs), and a framework analysis to develop a unified MFA strategy and a prototype for academic institutions. The SLR follows Kitchenham's methodology [Kit04], encompassing identification, evaluation, and synthesis of relevant literature on MFA technologies in both commercial and academic settings. To complement these findings with practical insights, semi-structured interviews [Ada15] are conducted with IT security experts from TU Wien and other Austrian universities. Using Kallio et al.'s five-step framework [KPJK16], three different interview guides are developed, allowing for tailored interviews with internal and external experts, focusing on either organizational or technical aspects. The results from both, the SLR and the

[1] Keycloak: `https://www.keycloak.org`. Accessed: 2024-10-20

SSIs, are analyzed using the framework analysis method [ST08]. This is a structured method for systematically categorizing and interpreting qualitative data. Additionally, as part of the framework analysis' final interpretation step, a practical demonstration of Keycloak was conducted. The implementation of this prototype served to validate the proposed strategy of the framework analysis.

1.4 Structure of the Thesis

Concerning the structure of the paper, the remainder of this thesis is organized as follows. Chapter 2 presents the related work using a systematic literature review that examines current MFA technologies, their application in academic and commercial settings, and identifies existing research gaps. In chapter 3, the methodology and findings from semi-structured expert interviews are discussed. This offers practical insights into the challenges and considerations for MFA implementation in academic environments. Here, TU Wien acts as a case study by interviewing both internal experts and stakeholders from external Austrian universities. Chapter 4 then applies the framework analysis research method to synthesize the insights from both the literature review and the interviews to develop a conceptual strategy for a unified MFA system. In chapter 5, a prototype for implementing MFA with Keycloak in academic environments is demonstrated. Finally, chapter 6 concludes the thesis by summarizing the key findings, while chapter 7 outlines directions for future work.

CHAPTER 2

Systematic Literature Review

A comprehensive review of existing literature on MFA technologies, their implementation in both commercial and academic settings with related impacts on user behaviour and security provides necessary background information about related work for further steps.

The Systematic Literature Review (SLR) is applied using the three main steps Identification, Evaluation and Synthesis. Kitchenham describes this methodology in-depth, guiding researchers in reviewing existing literature [Kit04]. First, relevant literature will be identified using specific search engines that redirect to academic databases. Afterwards, selected papers will be evaluated for their relevance and quality. A final synthesis will then summarize the findings to, first, identify similarities or gaps in the existing research and, second, derive potential solutions for the development of a conceptual framework by linking the key findings to the research questions.

2.1 Identification

This first step involves defining the scope for the systematic literature review. Next, the scientific databases as well as the search keywords that will be used to prompt for papers will be listed.

2.1.1 Scope

The research questions effectively represent the scope of the systematic literature review:

What technical and user acceptance challenges must be considered when implementing a unified MFA system in an academic environment, and how do these challenges differ from those in other types of organizations?

How can MFA systems be tailored to meet the specific needs and constraints of higher-education environments while ensuring high user adoption?

What role can Keycloak, an open-source identity and access management solution, play in the architecture of a robust MFA system designed for educational environments?

Based on these research questions, search keywords will be defined in the next section.

2.1.2 Search Keywords

In order to cover the entire scope, the following keywords will be used:

- Identity Management
- Higher Education
- Multi-Factor Authentication
- User Acceptance
- Keycloak

These keywords will then be combined to form optimal search inputs. In theory, the desired combinations are "Identity Management AND Higher Education", "Multi-Factor Authentication AND Higher Education", "User Acceptance AND Multi-Factor Authentication", and "Keycloak". However, due to diverse input masks and significant differences in result sizes of the various databases, the actual combinations of keywords used for each database was set individually. The actual combinations with the resulting numbers of papers is documented below in section 2.2.2.

2.1.3 Scientific Database

Four reputable scientific databases were selected to ensure comprehensive coverage of relevant studies. IEEE Xplore[1], ACM Digital Library[2], Springer Link[3], and Scopus (Elsevier)[4] were selected due to their listings of high-quality papers in the fields of computer science, engineering, and information technology.

[1]IEEE Xplore: https://ieeexplore.ieee.org/Xplore/home.jsp. Accessed: 2025-03-02
[2]ACM Digital Library: https://dl.acm.org. Accessed: 2025-03-02
[3]SPRINGER NATURE Link: https://link.springer.com. Accessed: 2025-03-02
[4]Scopus Preview: https://www.scopus.com/home.uri. Accessed: 2025-03-02

2.2 Evaluation

This section first describes the steps that were necessary to filter the large number of results and select a manageable set of papers. Furthermore, the query results of the four scientific databases are documented below.

2.2.1 Steps for Selection of Papers

There were three major steps for the inclusion and exclusion of papers:

First, a keyword based search on IEEE Xplore, ACM Digital Library, Springer Link and Scopus using filters for relevancy (e.g., written in English or German, published after the year 2010). This SLR focuses on more recent papers, as authentication processes evolved a lot and this thesis aims at analyzing the current state of the art in the context of MFA. The resulting numbers of found papers are documented below in Table 2.1. In total, around 1228 papers were found using this step.

Secondly, based on the results of these keyword based searches on the scientific databases, a manual selection of papers followed. This included assessing the relevance of the title and the abstract (if necessary), and the checking of the availability of a free version for TU Wien students. Out of the total 1228 papers from the first step, 47 papers were selected and then listed in an Excel Spreadsheet, where further filtering was applied.

Finally, after screening / reading the selected papers, another manual selection helped to find a final list of papers, that would be synthesized in the third step of the SLR. Here, the approach was to rate the papers using two inclusion criteria. First, a quality score was assessed, based on the number of citations and the recency of the publication. Then, a contextual relevance score was created to show how well a paper addresses the research questions. Here, the context was split into the four groups Identity Management - Academic Environment, Identity Management - General, Keycloak, and User Adoption. This last step resulted in the final selection of 20 papers, which are cited in the synthesis, section 2.3.

2.2.2 Documentation

The SLR was documented with the help of Microsoft Excel and Zotero. Potential papers were stored in Zotero collections to organize them into inclusion and exclusion lists, and also to export them to BibTeX. Excel was then used to document the resulting numbers of the databases, as well as the manual selection of papers. Table 2.1 below shows the results of the keyword based searches on the four scientific databases.

Database	Search Date	Combination of Search Keywords	Number of Results	Search In
IEEE Xplore	24.06.24	Keycloak	9	Anywhere
ACM Digital Library	24.06.24	Keycloak	101	Anywhere
Springer Link	24.06.24	Keycloak	160	Anywhere
Scopus (Elsevier)	08.07.24	Keycloak	33	Anywhere
IEEE Xplore	14.07.24	Identity Management AND Higher Education	24	Title, Abstract
ACM Digital Library	14.07.24	Identity Management AND Higher Education	124	Title, Abstract
Springer Link	15.07.24	"Identity Management" + "Higher Education"	429	Anywhere
Scopus (Elsevier)	15.07.24	"Identity Management" AND "Higher Education"	64	Title, Abstract, Keywords
IEEE Xplore	16.07.24	Multi-Factor Authentication AND Higher Education	9	Anywhere
ACM Digital Library	16.07.24	Multi-Factor Authentication	119	Title, Abstract
Springer Link	16.07.24	"Multi-Factor Authentication" + "Higher Education"	41	Anywhere
Scopus (Elsevier)	16.07.24	multi AND factor AND authentication AND higher AND education	11	Title, Abstract, Keywords
IEEE Xplore	17.07.24	User Acceptance AND Multi-Factor Authentication	19	Anywhere
Springer Link	17.07.24	"User Acceptance" + "Multi-Factor Authentication"	53	Anywhere
Scopus (Elsevier)	17.07.24	user AND acceptance AND multi AND factor AND authentication	32	Title, Abstract, Keywords

Table 2.1: SLR: Results of keyword based search, using scientific databases.

2.3 Synthesis

Key findings of individual papers are extracted and summarized. Similar studies are clustered into four groups (Identity Management - Academic Environment, Identity Management - General, Keycloak, and User Adoption), where findings are compared and discussed. This aligns well with Webster and Watson [WW02], who recommend to organize the review around themes, in order to follow a concept-centric approach. Also, following their guide, identified gaps in the current research are addressed, and finally results are linked to the research questions.

2.3.1 Key Findings of the Individual Papers

Identity Management in Academic Environments

To start with, Shchokin et al. [STK+24] provide an overview of digitalization trends in higher education. Although their paper does not directly address identity management, it underscores the increasing reliance on digital tools. Their study shows the rapid growth and potential of online learning platforms, which ultimately leads to an increasing demand in secure identity management solutions.

Kasahara and Shimayoshi [KS22] present their design and implementation of MFA deployments for Microsoft 365 (M365) in Kyushu University. Here are some key findings that might be relevant to enabling MFA for M365 implementations in general:

- Multi-factor authentication functionality provided by Azure AD (Active Directory, today known as Microsoft Entra ID) limits users' abilities to control MFA settings. For more flexible solutions, where users can register their MFA information themselves, the sole utilization of Azure AD might not be sufficient in M365 environments.

- In order to allow for risk-based conditional access (e.g., based on user location or device type) via Azure AD (i.e., Entra ID) premium P2 licenses are required. An effective implementation at Kyushu University relied on these licenses.
- Kasahara and Shimayoshi rolled out an initial voluntary MFA enrollment period, where users were allowed to self-enroll in MFA at their convenience. For this purpose, a self-enrollment system was designed using Microsoft Forms, Power Automate, and in-house web applications.
- Resistance against mandatory enforcement of MFA not only from students but also from executives or board members is common. The final deployment of MFA to all students was delayed repeatedly at Kyushu University. As of the paper's writing, MFA had not yet been mandated to all users, but around 500 users had voluntarily enabled it.

Similar to Kasahara and Shimayoshi, Nemoto et al. [NMA23] present the renewal of the academic information infrastructure of the Tokyo University of Agriculture and Technology (TUAT). The university replaced the previous on-premise authentication system with an Identity as a Service (IDaaS) system called Extic by ExGen Networks[5]. This enabled new features such as SSO and MFA. Here are some key findings of their implementation and initial operation:

- This IDaaS provider, Extic, can be integrated with key services, including Google Workspace, Microsoft 365, Zoom, and Moodle.
- Incorrectly stored IDs and passwords stored in browsers can lead to a significant number of authentication failures when switching to a new identity management system. Student training and proper communication is needed to remove these impediments.
- At TUAT, a gradual adoption of MFA was implemented as well. The IDaaS was introduced in 2021, and MFA became mandatory for all users by August 2022.
- The two given options to authenticate were either Time-based One-Time Password (TOTP) via a mobile app or Mail-based One-Time Password (MOTP). Of the two options, the majority of students chose MOTP.

Fidas et al. [FBPP21] discuss challenges and approaches to utilize biometric-driven data for student identity management:

- Biometric solutions, such as face, voice, and interaction-based authentication, became especially relevant during the COVID-19 pandemic, due to the shift to online learning. They can provide advantages over traditional methods, mostly improving usability.

[5]Extic by ExGen Networks: `https://www.exgen.co.jp/extic/`. Accessed: 2024-09-13

- The use of continuous authentication (e.g., tracking user behaviour during online learning activities) is particularly relevant for academic integrity in remote learning environments.
- Storage and handling of biometric data can expose sensitive personal information (e.g., ethnicity or health), raising privacy concerns.
- Certain biometric data, such as fingerprints or faces, are not secret, in a sense that they can be obtained from public sources, potentially leading to security breaches.
- Unlike passwords, biometric data cannot easily be changed if compromised.
- Privacy-preserving approaches for biometric-driven data authentication recommended by Fidas et al. include homomorphic encryption, blockchain technologies, and protocol-based methods such as secure multiparty computation or zero knowledge proofs to protect biometric data.

Constantinides et al. [CFS+23] present a framework called TRUSTID, which was developed as part of the ERASMUS+ 2020 programme. The framework provides a continuous identity management solution for students engaged in online academic activities, such as taking exams. In the scenario of an online exam, traditional systems often verify a user's identity only at the login or beginning of the exam, and then monitor students' activity manually via video conference by a supervisor. TRUSTID goes beyond this by continuously verifying the user's identity throughout their session using face and voice recognition. While the framework is related to the research questions, by adding an additional factor (MFA) to continuous identity management, it does not directly address the problem of this thesis' topic, which is the implementation of a unified MFA solution (used to login students and staff).

Blockchain Applications Hu et al. [HPTK23] inspect the current state of the art of blockchain applications in higher education institutions. These are the results of their systematic literature review:

- Blockchain technology is gaining traction in higher education institutions to address authentication issues with its decentralized, secure, and transparent nature.
- Potential use cases of blockchain in education include the issuance and verification of academic records (e.g., certificates, diplomas) using digital credentials. Furthermore, smart contracts could automate various administrative tasks, such as course registrations, fee payments, and scholarship distributions. However, these use cases are not relevant to the research questions of this thesis.
- Traditional identity management could be reshaped using blockchain technology with the introduction of self-sovereign identity (SSI) management. This approach

enables students and staff to manage their personal data without relying on centralized authorities. Yildiz et al. [YRN+21] implemented a proof-of-concept using SSI for decentralized identity management at TU Berlin, as summarized below.

- Challenges in implementing blockchain include the complexity of integrating with existing academic infrastructures, as well as regulatory and legal issues, as there is a lack of regulations and standards.

Based on the advent of blockchain technologies, Yildiz et al. [YRN+21] present another type of modern authentication. They connect self-sovereign identity with "traditional" federated, SAML-based authentication. Self-sovereign identities are digital identities that are stored in a decentralized approach, e.g., with the use of blockchains. Users can control and manage these identities (that they own) without relying on centralized identity providers, e.g., from Google, Microsoft or Apple. The verifiable credentials of the users are held in personal wallets that give them full control over their identity data. Key findings related to MFA or identity management in academic environments include:

- SSI can be integrated with existing federated identity management systems of higher education environments, as a proof-of-concept implementation of the authors at the Technische Universität Berlin shows. In this scenario, a hybrid approach allowed students to authenticate using SSI credentials while still maintaining compatibility with the existing SAML-based authentication workflows. This means that both, identity providers (i.e., federated authentication) and SSI, co-exist and can be used alongside, allowing for a less disruptive transition. Ultimately, an adoption to using SSI without identity providers is desired.
- Still, a transition to SSI requires significant infrastructure changes, as it moves from traditional account-based models to relationship-based models that use decentralized public key infrastructures (DPKI).
- While SSI aims to increase security by decentralizing identity management (e.g., no more risks of identity theft through attacks on identity providers), it still requires robust security measures for verification and communication.

Identity Management in a General Context

Midhuna and Jeyanthi [RJ23] delve into modern authentication methods, providing an overview about identity management in general:

- The usage of single-factor authentication (i.e., traditional password based authentication) should be limited due to various security risks. Cloud-based systems need to be prepared to withstand increasingly sophisticated cyber criminality that applies brute force, phishing, replay attacks, etc.
- As a result, Midhuna and Jeyanthi explain a growing shift towards passwordless authentication, using e.g., biometrics, public key infrastructure (PKI) certificates, or FIDO2 keys.
- Continuous authentication, which monitors user behaviour in real-time, is a supplementary technique. It can detect anomalies based on patterns like keystroke dynamics or mouse movements, and is a method, especially useful in environments where access needs to be constantly verified.
- MFA still faces challenges like social engineering attacks or vulnerabilities related to SIM swapping and man-in-the-middle attacks.
- Digital certificates combined with PKI-based authentication are often used in enterprise and government systems. Even though the combination of PKI and biometric data is being considered a robust mechanism, man-in-the middle attacks still remain a concern.
- Adaptive authentication is another passwordless technique that can be incorporated to establish secure authentication systems. It adjusts the authentication process based on the context (e.g., location, device, time).

Al Saleem and Alshoshan [AA21] propose a novel multi-factor authentication system designed to enhance security while being cost-effective and user-friendly. The system uses graphical passwords as additional factor of authentication, next to other common factors like username and password. The following key findings could be identified:

- The graphical passwords applied by Al Saleem and Alshoshan are a knowledge-based authentication method where users select a sequence of images during registration. During login, users must then identity the correct images in the proper order.
- This approach does not rely on secondary devices (that offer biometric hardware or run third party applications) or SMS services, resulting in lower implementation and operating costs.

Keycloak

To start with, a direct quote from Karol Nowak [Now23] summarizes the potential of Keycloak to be a significant part of this thesis' proposed identity and access management (IAM) solution for the case study at TU Wien:

> "Organizations with multiple applications often struggle to manage user authentication and access control across their diverse application landscape. Keycloak can help centralize IAM by acting as the single point of authentication and access control for all applications, simplifying the management of user accounts and permissions while providing a seamless user experience."

Divyabharathi and Cholli [DC20] provide a review on Keycloak:

- Keycloak is an open-source identity and access management system that provides a centralized platform for user management, (multi-factor) authentication, and single sign-on (SSO).
- Keycloak can integrate with various external identity management systems like Active Directory or generally the internet protocol LDAP. It supports industry-standard frameworks and protocols, including OAuth 2.0, OpenID Connect and SAML 2.0, enabling federated identities.
- The paper compares Keycloak with other identity management systems, WSO2 Identity Server and Shibboleth. Keycloak's support for OpenID Connect, ease of configuration, and use of WildFly middleware are highlighted as advantages over WS02, which is considered harder to configure.
- Two-factor authentication via time-based one-time password (TOTP) or HMAC-based one-time password (HOTP) is supported through apps like Google Authenticator and FreeOTP.
- Divyabharathi and Cholli also emphasize Keycloak's active community, which contributes to regular updates, ensuring that Keycloak is a modern and secure solution for identity management.

Anderson and Keahey [AK22] describe the migration of Chameleon[6] from a proprietary identity management solution to an architecture supporting SSO and federated identity. This architecture contains Keycloak as the main identity and access management system, providing authentication and session management. The following key findings can be identified from their migration:

[6] Chameleon: `https://www.chameleoncloud.org`. Accessed: 2024-09-15

- Similar to other migrations reviewed in this SLR, Chameleon also provided a self-migration tool to their thousands of users to allow them to transfer their credentials from the legacy system to the new one.
- Keycloak was used to delegate authentication to multiple external identity providers through OpenID Connect and SAML, enabling SSO across different platforms.
- Keycloak's centralized session management and authorization policies enabled Chameleon to implement role-based access control for different applications.

Baun et al. [BKCK24] present insights to a platform for creating and using complex virtualized IT structures at Frankfurt University of Sciences, that is used for teaching and research purposes. They employ Keycloak as the authentication service within the platform. It is used to connect the platform to the university's central authentication system, as well as managing access to all individual resources of the platform infrastructure (e.g., virtual machines and networks). In this implementation, Keycloak also enables extending authentication to external service providers, such as Amazon Web Services and Google Cloud Platform using the User-Managed Access (UMA) protocol.

Preuveneers et al. [PJJ21] introduce a framework called AuthGuide to assist security administrators in configuring MFA on top of Keycloak. The framework helps to analyze the trade-offs between security, privacy, and usability when selecting and configuring different authentication factors by guiding administrators through a series of questions. It also validates these configurations against industry standards (NIST SP 800-63B). While the framework was developed and validated on top of Keycloak by researchers at KU Leuven as part of an academic project, unfortunately, the actual framework is not publicly available as an open-source tool. However, here are some of the key insights they found using AuthGuide to balance security, privacy, and usability:

- The ability to handle different MFA configurations, such as fixed authentication factors (e.g., passwords with one-time passwords) and flexible authentication factors (users can choose which factors to use, e.g., biometrics or contextual factors like location) is crucial for organizations that need to accommodate a wide variety of user preferences.
- Context-based authentication (e.g., using location or browser fingerprinting) enhances security, but can infringe on user privacy.
- Biometric authentication methods (e.g., fingerprints or facial recognition) are convenient for users and maintain privacy by keeping biometric data on a user's device. On the other hand, however, they raise concerns about security, as the authenticating party must trust the client, i.e., mobile phones, where false positive rates can vary and are not known for every mobile device.

Thorgersen and Silva [TS21], both active members of the development and leadership team of Keycloak, wrote a book that introduces potential developers, system admins, or security engineers to Keycloak. The book first provides comprehensive guidance on installing and running Keycloak on various platforms, as well as setting up realms, users, groups and roles using the Keycloak admin console. In the second section, it explains essential concepts like OAuth 2.0, OpenID Connect and SAML 2.0, and how to use them with Keycloak to secure applications. The third section covers deploying Keycloak for production environments, and integrating Active Directory, LDAP and other third-party identity providers. Furthermore, this section covers user authentication flows, such as using passwords, OTP, and WebAuthn, which are relevant for MFA setups. The last section provides some security considerations, such as encrypting communication and securing users, databases and applications. Some key findings (that have not been mentioned before in other papers) are:

- Keycloak is implemented in Java and can therefore be run on any operating system that has a Java virtual machine installed, without the need to install any additional dependencies.
- It uses JSON Web Signature (JWS) with JSON Web Tokens (JWT) as the default token format.
- This book demonstrates many useful configurations for Keycloak step by step, which might be very beneficial for the setup of a prototype or an actual implementation for the case study at TU Wien.

Christie et al. [CAS+17] show the practical relevance of Keycloak in modern identity and access management solutions, by replacing WS02 Identity Server with Keycloak in the Apache Airavata[7] middleware, which powers science gateways. The following list summarized the main takeaways:

- Keycloak's support for OpenID Connect and SAML allowed for authentication with federated identity providers. This included an integration with CILogon[8], a federated authentication service used by many academic institutions, to provide SSO across science gateway applications. This integration ensured that users could log in with their institutional credentials, without needing to interact with Keycloak's user interface (login screen) directly, reducing confusion and improving the user experience.
- Keycloak's REST API plays a crucial role in allowing administrators to manage user roles and access control (RBAC) dynamically. With Airavata middleware, an abstraction layer was developed to interact with Keycloak (API) indirectly, to

[7]Apache Airavata: `https://airavata.apache.org`. Accessed: 2024-10-18
[8]CILogon: `https://www.cilogon.org`. Accessed: 2024-10-18

promote modularity and avoid vendor lock-in, i.e., allow for replacing Keycloak with another system, if needed.

- Keycloak does not support XACML. Christie et al. instead used the Keycloak REST API to make access control decisions.

El Hajj Hussein experimented with integrating Keycloak with different types of applications at CERN, as published in a technical report [EHH19] from 2019. The motivator for this project was a planned migration from commercial software to open-source solutions (using Keycloak for authentication) of all CERN services due to rising license costs. The author intended to create reproducible examples demonstrating and documenting Keycloak configurations for web, mobile and desktop applications, with varying programming languages. Here are some key findings:

- Keycloak supports all three OpenID Connect authentication flows: Authorization Code Flow, Implicit Flow, and Hybrid Flow.
- The reproducibility of the examples is very limited, as the Git repository is restricted to CERN users.
- The author wanted to develop a device flow pluggable authentication module (PAM), but the necessary OAuth 2.0 flow was not supported by Keycloak back then. As of today, since Keycloak version 13.0.0, this support for OAuth 2.0 Device Authorization Grant is available[9].
- The report concludes by stating, that the documentation and availability of libraries for Keycloak is not sufficient. This seems to have changed in the last years since 2019.

Not directly related to the report by Hussein, in 2022, CERN implemented mandatory 2FA for all users with access to critical services, as presented by Ahmad et al. [ACS+24]. CERN had previously introduced an optional 2FA system in 2019, but adoption was low. Their SSO system, Keycloak, required managing separate realms for the optional 2FA, which led to duplicated users. This and a severely alerting simulated phishing campaign (where 2000 users gave away their passwords), led to the migration to an "always-on" 2FA approach with a simplified login flow with just one Keycloak realm. This new login flow mandates the use of a TOTP (Time-based One-Time Password) or WebAuthn token for all critical accounts. The main takeaway from this article is that Keycloak allows for the implementation of Service Provider Interfaces (SPI)[10], that enable customized configurations. E.g., Ahmad et al. added a custom role in the user token and modified

[9] Keycloak Release Notes, Version 13.0.0: `https://www.keycloak.org/docs/latest/release_notes/index.html#keycloak-13-0-0`. Accessed: 2024-10-19

[10] Keycloak Service Provider Interfaces: `https://www.keycloak.org/docs/26.0.0/server_development/#_providers`. Accessed: 2024-10-20

the default authentication flow to add custom checks and verifications before users log in. These custom extensions helped them in migration phases from the legacy flow to the new 2FA flow.

User Adoption

In their study about how mandatory second factor authentication affects user experience, Abbott & Patil [AP20] present the following findings:

- While two-factor authentication (2FA) is effective in enhancing security, its mandatory use can degrade the user experience, particularly when applied to all systems. Users find 2FA acceptable when it is limited to sensitive systems only, and not necessary for every login.
- Smartphone push notifications are the preferred type of second factor, followed by text messages and physical hardware tokens.
- Mandatory 2FA for all systems increase frustration and decrease satisfaction. Only users who opt into 2FA voluntarily report a better overall experience.
- The study suggests that 2FA implementation in universities should focus on balancing security with user convenience to avoid security fatigue. Especially in academic settings where multiple logins are required daily, limiting 2FA to sensitive systems and allowing voluntary opt-ins for other systems may reduce the user burden, while still maintaining high security standards.

Arnold et al [ABG+22] analyse the emotional impact of multi-factor authentication for university students. These are their key findings:

- The results of their user study indicate that the emotional impact of MFA is significant, with students reporting feelings of frustration, stress, and anxiety towards MFA that is used for time-sensitive tasks (e.g., quizzes and exams).
- In their study, 57.6% of students reported that MFA had prevented them from completing at least one time-sensitive task.
- The negative emotions are correlated with a lack of belief in MFA's worth and its perceived security benefits. 38.1% of students believed that the additional effort of MFA was worth the increase in security.
- The emotional burden can be reduced, for example, by disabling MFA during class time or when students are on the campus WiFi.
- If students feel that the security burden from MFA is too high, they may try to reduce their perceived inconvenience by using weaker passwords instead. Hence, clear communication on both sides is important to discuss the personal security benefits of MFA.

2.3.2 Clustering and Analysis of Findings

The findings have been assigned to four clusters: Identity Management - Academic Environment, Identity Management - General, Keycloak, and User Adoption. This will help to address the research questions more efficiently.

Identity Management - Academic Environment

Across the reviewed literature on identity management in the context of academic environments, two primary trends are evident: The increasing reliance on MFA and a shift towards innovative identity management methods, such as biometrics and blockchain. MFA is being implemented to address the growing security needs, but institutions face challenges with adoption due to user resistance, especially when MFA is mandatory. Implementations at Kyushu University and Tokyo University of Agriculture and Technology show that flexible MFA systems, which allow for user-driven enrollment, and gradual transitions to enforcing MFA are often necessary.

Identification of Gaps:

- Even though the transition to decentralized identity, using blockchain and SSI, present promising developments, there is still a significant gap in understanding the practical challenges of integrating these technologies with existing academic systems. Further studies are needed to explore cost-effective, less disruptive (actually feasible) integration strategies.
- Most approaches for implementing MFA are institution-specific, lacking a unified framework that could be widely adopted across higher education institutions. This gap calls for research into developing MFA adoption strategies specifically to the needs of academic environments.

Identity Management - General

Similar to reviewed literature on identity management with a focus on academic environments, the two papers in the general context also reveal a shift towards multi-factor authentication and passwordless methods to address the limitations of single-factor authentication. Mentioned modern methods for additional factors are biometrics, public key infrastructure certificates, FIDO2 keys, continuous authentication, adaptive authentication, and graphical passwords.

Identification of Gaps:

There is only limited research on the feasibility and practical readiness of some of the mentioned authentication methods, especially graphical passwords. Based on the selected papers, more information is needed to assess the usability and robustness on continuous and adaptive authentication as well.

Keycloak

The reviewed literature presents Keycloak as a highly flexible and adaptable open-source identity and access management solution suitable for managing multi-factor authentication (MFA), single sign-on (SSO), and centralized authentication. Keycloak's support for industry-standard protocols like OAuth 2.0, OpenID Connect, and SAML allows seamless integration with external identity providers, such as Active Directory, and LDAP. Studies emphasize its effectiveness in providing centralized session management and role-based access control, making it a robust option for diverse academic environments. Keycloak's flexibility also extends to configuring MFA with features like context-based authentication, authenticator apps (e.g., Google Authenticator), and support for various authentication flows. However, when migrating from complex legacy systems towards MFA and Keycloak, gradual deployments, possibly by implementing self-service tools for enrollment and migration, are needed to ensure smooth transitions.

Identification of Gaps:

- Although Keycloak has been deployed successfully in various environments, there is limited empirical research on its scalability and performance in large-scale deployments, particularly in higher education settings.
- Keycloak's flexibility in supporting customized configurations introduces potential security risks (e.g., through improper implementation of Service Provider Interfaces). There is a gap in research on best practices for securely configuring these customizable elements.

User Acceptance

All key findings in this cluster highlight that MFA poses significant challenges related to user experience. Mandatory MFA often leads to frustration, stress, and security fatigue, especially when applied universally across all systems. Users prefer MFA for sensitive systems only, as frequent logins increase the burden. To maintain a positive user experience, it is beneficial to balance security with usability, allowing voluntary opt-ins or context-based exemptions.

Identification of Gaps:

Both studies indicate that user resistance to MFA is partly due to a lack of understanding of its benefits. Further research is needed to explore effective communication strategies, that can help users appreciate the importance of MFA, and their effectiveness/feasibility.

2.3.3 Linking of Results to Research Questions

Research Question 1: *What technical and user acceptance challenges must be considered when implementing a unified MFA system in an academic environment, and how do these challenges differ from those in other types of organizations?*

Implementing a unified MFA system in an academic environment presents challenges like scalability, user acceptance, and integration with potentially very complex legacy systems, comprising a multitude of different applications. Unlike other organizations, academic environments have diverse user groups and frequent changes in user populations. This requires flexible and scalable solutions. User acceptance is particularly challenging due to resistance from students, who often think that the burden from mandatory MFA is too high. Addressing these challenges requires a balance between security and convenience, if possible. Potential strategies include voluntary opt-ins (especially for migration phases) and context-based authentication to reduce the strictness of mandatory MFA.

Research Question 2: *How can MFA systems be tailored to meet the specific needs and constraints of higher-education environments while ensuring high user adoption?*

To tailor MFA systems for higher-education environments, flexibility and user-centric designs are important. Similar to the answer to research question 1, allowing voluntary MFA enrollment, providing multiple authentication options (e.g., authenticator apps, context-based and adaptive authentication), and limiting MFA to sensitive systems is likely to enhance user adoption. Additionally, effective communication and training is necessary to help users understand the importance of MFA. Furthermore, to meet the technical needs and constraints of universities, an IAM solution like Keycloak can be implemented to provide centralized identity management and flexible integration with existing systems and third party providers.

Research Question 3: *What role can Keycloak, an open-source identity and access management solution, play in the architecture of a robust MFA system designed for educational environments?*

Keycloak can serve as the central component in the MFA system by providing identity management, centralized session control, and integration with existing systems like Active Directory and LDAP. Its support for industry-standard protocols (OAuth 2.0, OpenID Connect, SAML) and customization capabilities make it well-suited for addressing the diverse authentication needs of academic institutions. More details to answer this research question will follow after conducting the semi-structured expert interviews.

CHAPTER 3

Semi-Structured Expert Interviews

Engagement with IT security experts and other stakeholders at TU Wien and other Austrian universities will provide insights into practical challenges and considerations for implementing effective MFA solutions. This qualitative research step will follow the methodology of semi-structured interviews (SSIs) [Ada15]. Sampling will be used to select interview participants from the three universities, based on their expertise and involvement in security and identity management. An interview guide will then be created, containing a mixture of open- and closed-ended questions, covering topics such as current authentication practices, perceived barriers, and potential solutions. Kallio et al. [KPJK16] provide a five-step framework to create such a semi-structured interview guide, which I will follow. The interviews will then be conducted either face-to-face or via video conferencing, recorded, and transcribed to allow for a comprehensive data analysis.

3.1 Development of Semi-Structured Interview Guide

The development of the interview guide follows the five phases presented by Kallio et al. The phases are the identification of prerequisites, retrieving and using previous knowledge, formulating the preliminary interview guide, pilot testing this interview guide, and eventually, finalizing the interview guide.

3.1.1 Identifying the Prerequisites

First, the appropriateness of this method (Semi-Structured Interviews) has to be established. Findings from the SLR highlight the complexity of implementing MFA within academic institutions. Challenges such as user resistance, integration with legacy systems, and scalability were evident in case studies from universities like Kyushu University and

TUAT. The SLR also emphasized that while MFA is being progressively adopted in higher education, mandatory implementation can lead to frustration and security fatigue among users. Furthermore, Keycloak was identified to potentially act as a centralized IAM solution.

These insights should make SSIs a suitable method to explore perspectives of IT security experts, as the interviews allow for the investigation of technical/administrative aspects of existing MFA implementations in Austrian universities. They can help to deepen the knowledge from the SLR insights. The qualitative data gathered through these practical insights will help to identify best practices and to develop a strategy for a unified MFA system implementation.

3.1.2 Retrieving and Using Previous Knowledge

The systematic literature review built this required knowledge base that is now used for the development of the preliminary interview guide. The insights were retrieved in the synthesis section 2.3 of the SLR and will be used to create the 6 themes, as can be seen in the following section.

3.1.3 Formulating the Preliminary Interview Guide

An SSI interview guide consists of main themes and follow-up questions. In the preliminary interview guide, I created 6 sections. Each section has one main theme (question) and multiple follow-up questions, with the exception of the first section, which has two main themes. If the interviewee addresses the subtopics of the follow-up questions in their initial response, the follow-up questions will not be needed. The sections are background & current practices, implementation process, Keycloak, user adoption, lessons learned, and recommendations for TU Wien.

The resulting preliminary interview guide is listed in the appendix under Preliminary Interview Guide.

3.1.4 Pilot Testing the Interview Guide

The pilot testing of the preliminary interview guide involved two key stages. Initially, valuable feedback was obtained from Prof. Eidenberger, which helped refine the structure and clarity of the interview questions. Based on this feedback, the interview guide was finalized.

Additionally, the two internal interviews at TU Wien also served as a practical pilot run. This allowed for further discussion and eventual adaption of the guide.

3.1.5 Finalizing the Interview Guide

In this fifth step of the interview guide development process, the interview guide was refined by incorporating feedback from Prof. Eidenberger. His input led to the creation

of two separate guides. The interview guide was split into two separate guides for organizational and technical interview partners, ensuring that each group is addressed with relevant and specific questions. Additionally, recommendations originally framed exclusively for TU Wien were re-framed into more general advice applicable to universities. This way, any potential discomfort related to giving direct recommendations to other Universities is mitigated. Finally, the scenario at TU Wien was introduced earlier in the interview to provide better context for the discussion.

Prior to the Start of the Interview Questions

Prior to the actual start of the interviews, a brief overview of the current state of identity management at TU Wien is provided to the interviewee:

At TU Wien, identity management involves different mechanisms for the main student platform, network, and mail accounts. The main student platform enables optional 2FA which is barely utilized by students. The university is considering a unified MFA approach that uses Keycloak as the central IAM solution.

Splitting the Interview Guide

After the final review, the internal guide was split for three different types of interviewees. First, for interviews conducted directly at TU Wien, the Internal Interview Guide was created with the goal of establishing the necessary understanding of the current state of Identity & Access Management at TU Wien. This guide focuses on gathering insights into the university's existing authentication mechanisms, challenges, and future plans.

To complement this, two external interview guides were developed for interviews with experts from other Austrian universities. These guides aim to gather knowledge and best practices from diverse perspectives. Specifically:

1. The Organizational Interview Guide targets interviewees with organizational expertise, focusing on policies, user adoption strategies, and administrative challenges related to IAM.
2. The Technical Interview Guide is designed for interviewees with a technical focus, addressing infrastructure, system integration, and technical challenges of implementing MFA and other authentication mechanisms.

Both external guides are adaptable and can be combined during a single interview, which aligns well with the flexible nature of Semi-Structured Interviews.

3.2 Results of the Completed Interviews

This section shows the results of the completed interviews, split into two internal and three external expert interviews. The internal interviews refer to experts at TU Wien, the external interviewees are experts at other Austrian universities.

3.2.1 Internal Interviews

Interview 1: Head of Campus IT

a. How are identities currently managed?

There are two central authentication paths: First, a Single Sign-On (SSO) system, referred to as the "Identity Provider", to which various services (e.g., the main student platform) are connected. Second, an Active Directory (AD) environment supporting several other systems (e.g., their data warehouse, Jira, Confluence, Exchange).

b. How many systems are there in total?

Estimated Number of Systems: Possibly 100 to 200 in total, including large university-wide services and smaller internal ones.

c. Which authentication mechanisms are currently used for these systems?

Single Sign-On (SAML 2.0) is being used for many web services (via the custom TU Wien Identity Provider). Next, AD-based authentication is especially important for on-premises Microsoft Exchange. Furthermore, a user-configurable second factor exists for the SSO system (though not mandatory for everyone), and geofencing is in place for the internal network: Access from outside the European Economic Area (EEA) requires VPN.

d. What, in your opinion, are the biggest challenges when introducing a unified MFA solution at TU Wien?

Technical Fragmentation: Some systems use SSO, others AD. Exchange On-Premise is not easily integrated with standard MFA tools because Microsoft (on-prem) does not provide an "out-of-the-box" 2FA solution.

User Acceptance: University environments often see significant pushback whenever changes are introduced. Many do not read emails or official announcements, which can lead to confusion and complaints. Proper information campaigns and training can mitigate these issues.

Vendor Lock-In & Cost: Commercial providers (like Cisco Duo) can implement a broad "Big Bang" approach via VPN-based MFA, but it can be expensive and locks the institution into a single vendor's solution. TU Wien leans toward open standards where feasible.

e. Are there any technical limitations within the current infrastructure?

On-premises Exchange is a major limitation. Microsoft does not natively support MFA in the on-premise scenario (unlike Azure-based Exchange Online). AD-based services are also fragmented, as some use SSO, whereas others do not. This could be fixed.

Implementing a single, universal MFA method is difficult due to these varied authentication backends.

f. Which concerns have students or staff raised regarding mandatory MFA?

The interviewee anticipates initial resistance from both students and staff. Complaints often arise about having to learn new processes, and many feel they have not been adequately informed (even if information emails were sent). However, with proper communication, training videos, and local IT support, the interviewee believes acceptance will grow over time.

g. How do you plan to reconcile security and user-friendliness when implementing a potential MFA solution?

The interviewee favors an easy-to-use solution and emphasizes education and training for users to reduce frustration and confusion. The importance of having as few distinct MFA apps or mechanisms as possible (to avoid user confusion about "which second factor" they should use).

h. How do you assess the feasibility and usefulness of context-based authentication, or limiting mandatory MFA to individual applications that require increased security?

Geofencing is already in place, restricting access from outside EEA unless via VPN. The interviewee indicated that additional context-based approaches, like requiring MFA only outside the TU network, are attractive but do not fully protect internal systems if an attacker gains internal access. They do see potential for limiting mandatory MFA to critical applications, although the long-term goal is to secure all major services. Exchange On-Prem, for instance, has unique technical obstacles.

i. Which central components of the current infrastructure would need to be adapted for implementing comprehensive MFA?

For the Single Sign-On (SAML Identity Provider) the goal would be to move as many services as possible towards SSO.

Next, the Active Directory environment needs to be consolidated (for services that do not / cannot use SSO). Microsoft Exchange On-Prem in particular poses a big challenge because it does not natively support MFA.

j. Would you recommend a big-bang approach or a gradual, iterative approach for the integration?

The interviewee strongly suggests iterative steps. A strict “Big Bang” approach might be possible with a commercial solution like Cisco Duo (enforcing VPN + MFA for all external access), but it is expensive and not aligned with open standards. Currently, TU Wien is rolling out changes step-by-step (e.g., geofencing first, then potentially MFA on VPN, etc.).

k. Do you consider Keycloak a suitable component for a planned MFA implementation?

The interviewee notes that the external university "A" successfully integrated Keycloak for MFA, but they do not have on-premise Exchange, which is the main sticking point at TU Wien. Because Exchange On-Prem does not integrate well with Keycloak, a purely Keycloak-based approach is problematic.

Currently, NetIQ[1] is also being analyzed as a potential new IAM solution.

l. Are there any specific challenges you would like to learn about from other universities’ implementations?

The interviewee does not specify additional major questions beyond the on-prem Exchange challenge and the desire to maintain data sovereignty (i.e., not relying too heavily on Microsoft or large proprietary vendors). They note that many Austrian institutions have simply moved Exchange to the cloud (thus enabling Azure MFA), but TU Wien wants to avoid that for data sovereignty reasons.

Potential shifts towards open source solutions like openDesk or Open-Xchange have been brought up briefly.

[1] NetIQ: `https://www.netiq.com/documentation/`. Accessed: 2025-03-02

Interview 2: Software Engineering Department Employee

a. How are identities currently managed?

First, there is a SAML 2 provider that is aligned with the ACOnet Federation (used by Austrian universities and related institutions).

Second, Active Directory (AD) / LDAP is being used for various Microsoft-related services (e.g., Exchange on-prem, other apps that do not support SAML).

b. How many systems are there in total?

The interviewee implies there are numerous applications (some are modern web apps needing OpenID Connect/OAuth, others are legacy SAML or AD-only).

c. Which authentication mechanisms are currently used for these systems?

SAML 2 (via a Simple-SAML-PHP Identity Provider) is used for many web-based services, including the ACOnet Federation.

AD/LDAP is used for Microsoft-centric services (e.g., on-prem Exchange, some other internal apps).

OpenID Connect / OAuth usage is emerging (or needed) for modern web front-ends (Angular, React, etc.), but not yet broadly implemented.

Geofencing for external (non-EU/EWR) access was mentioned.

d. What, in your opinion, are the biggest challenges when introducing a unified MFA solution at TU Wien?

Microsoft Exchange On-Prem does not provide an out-of-the-box MFA option. Outlook Web Access (OWA) is difficult to secure with typical open-source solutions.

Fragmented Authentication: Some systems use SAML, others rely on AD or LDAP only. Modern apps need OIDC; older ones still require SAML or AD.

User Confusion / Multiple Passwords: Currently, SAML and AD credentials are separate; a unified MFA must reconcile these.

Mapping Attributes: Any shift to a unified provider (e.g., Keycloak or NetIQ) must preserve user IDs and attributes across systems, or risk breaking existing logins.

e. Are there any technical limitations within the current infrastructure?

On-prem Exchange is repeatedly cited as a core limitation, as Microsoft actively pushes Azure-based solutions for MFA.

SAML Federation is necessary to maintain (ACOnet), but it is harder to integrate with modern web frameworks that typically rely on OIDC.

f. Which concerns have students or staff raised regarding mandatory MFA?

The interviewee assumes there will be concerns and some pushback. They emphasize that if MFA is made mandatory by the university's top management (Rektorat),

it must be firmly enforced without making too many exceptions. The interviewee suggests that it is "a necessary inconvenience."

g. How do you plan to reconcile security and user-friendliness when implementing a potential MFA solution?

The solution should be as transparent as possible and ideally unified (only one MFA mechanism/app if possible). Minimizing the number of separate second-factor apps or processes is key to user-friendliness. Ultimately, it must be communicated clearly—with strong top-level support—so that users accept it.

h. How do you assess the feasibility and usefulness of context-based authentication, or limiting mandatory MFA to individual applications that require increased security?

The interviewee questions whether network-based exemptions (e.g., no MFA needed on campus) truly enhance security, because Eduroam (campus WLAN) could be easily accessed by an attacker on-site. Furthermore, they mention that it is possible to exclude some apps from MFA by customizing the "authentication chain," but that approach can lead to an excess of exceptions and potential security gaps. Altogether, the interviewee generally favors a uniform approach for all apps unless a very compelling reason justifies an exception.

i. Would you recommend a big-bang approach or a gradual, iterative approach for the integration?

The interviewee leans toward a step-by-step (iterative) approach, with careful communication, to avoid confusion and user pushback. However, they mention that it depends on the solution chosen. Big-Bang is possible in theory (e.g., Cisco Duo enforced on all VPN access), but might be both expensive and unpopular if it creates friction.

j. Do you consider Keycloak a suitable component for a planned MFA implementation?

They see it as generally suitable for introducing MFA for most modern web services at TU Wien. However, on-prem Exchange integration is still problematic, and Keycloak does not solve that gap easily.

k. What specific advantages (or disadvantages) does Keycloak offer for TU Wien's use case?

The interviewee mentions the advantages of Keycloak being an open-source solution with large community support compared to proprietary NetIQ. With Keycloak it is easier to find ressources and information online for free. Furthermore, Keycloak can act as both an SAML IdP and an OIDC provider and it is easier to implement various MFA methods (FIDO2, WebAuthn, TOTP, etc.) "out of the box." However, the interviewee thinks that it is more important to consider protocols and system

architectures rather than specific tools, such as a selection between Keycloak or NetIQ.

l. Have any initial tests or evaluations of Keycloak already been conducted at TU Wien?

Keycloak is used in "campus software development" and test systems already. The interviewee references that other Austrian universities have done deeper Keycloak rollouts, but TU Wien is still exploring possibilities (alongside NetIQ).

m. Are there any specific challenges you would like to learn about from other universities' implementations?

The interviewee is interested in comparing how others manage the "Microsoft problem," i.e., MFA for Exchange On-Prem. They also want to see if and how other universities avoid vendor lock-in (e.g., going fully into Microsoft Azure).

3.2.2 External Interviews

The three external interviews were held at two different Austrian universities, here called "A" and "B".

Interview 3: Austrian University A

a. Do you use mandatory MFA at your University? If so, how long has your university been using it, and what were the initial motivations for implementing it?

Yes, they use mandatory MFA. It became mandatory in February 2024. They started the MFA project at the end of 2022, received official project approval, and implemented it so that by February 2024, it was required for all users.

The motivations were: Preventing phishing and stolen credentials. Password-based security alone was seen as insufficient, especially given frequent phishing attempts. The interviewee had tried to start an MFA project in 2019, but it did not receive high priority back then. By 2023/2024, top management gave full support, and the project got the necessary backing.

b. What organizational strategies were employed to roll out MFA smoothly?

They had a “gradual” or “evolutionary” approach, rather than a single big bang. First, they offered the possibility of MFA to users without making it mandatory. This allowed both users and the service desk to gain experience (how to reset second factors, handle forgotten factors, etc.). Then they introduced a “nag-screen” period (two weeks for each user) that reminded people to enable MFA. After that period, the user could not log in without setting up MFA. They also gave users the option to “trust their device,” meaning if someone logs in from the same device frequently (with Touch ID, etc.), they do not need repeated second-factor prompts.

c. What communication strategies were most effective in gaining acceptance by students and staff?

They created short videos and thorough documentation (screenshots, step-by-step guides), gave early demos to the student union (ÖH) to preempt concerns, and they offered workshops, though attendance was limited because "users often do not invest time in workshops". Also, they used the nag-screen approach and regular email communications.

d. How was the decision to implement mandatory MFA met? Were the students involved in this decision?

Some people were initially against it ("as with any security measure"), but the project team could argue its necessity easily (phishing risks, general industry standards). Also, they informed the student union (ÖH) early, which helped avoid conflicts.

Students were not the ones making the decision, but our university still tried to include them in discussions and show them the plans to reduce fear.

e. How do students and staff respond to mandatory MFA? Were there significant changes in user experience?

The interviewee says no significant "pushback" or "escalations" arose. They see it as "no big deal" for most people once they tried it—especially since the login process can even become more convenient with saved device trust or SSO tokens. Some staff/students initially worried about using personal devices, but the system accommodates different methods (e.g., no forced phone app if you don't want it).

f. What feedback or metrics have you gathered to evaluate user satisfaction and adoption rates, if any?

No formal feedback survey was carried out because the tight schedule would not allow changes to be implemented prior to go-live. However, they did measure how many users actually configured a second factor. The number matched their estimate of actively enrolled students, suggesting strong coverage.

g. Could you very briefly describe the current state of identity management and authentication mechanisms at your university?

University A uses Keycloak for central authentication and MFA. They also still have some legacy identity prodivers (e.g., SAML, E-Directory, AD). Furthermore, there is yet one more identity provider: Their Campus-Online system is a key source of "base accounts," which then must tie into Keycloak for MFA.

h. Can you walk me through the technical process of implementing MFA?

They already had Keycloak in place for some services, so extending it to MFA was natural. A pilot phase tested how Keycloak handled VPN (Cisco ASA), SAML, OIDC, etc.

i. What tools and mechanisms does your identity management solution consist of?

Keycloak is their primary IAM tool for MFA.

They allow multiple second-factor methods: TOTP apps, WebAuthn (Touch ID, Windows Hello, FIDO keys), and fallback recovery codes. They intentionally avoided sending codes via SMS or push-notification apps to mitigate "fatigue attacks."

j. What challenges did you face with infrastructure complexity and legacy systems?

They have a wide variety of legacy ID sources (AD, eDirectory, SAML), which all needed to integrate with Keycloak. One of the biggest leaps was changing the VPN authentication from simple RADIUS username/password to a web-based OIDC flow through Keycloak.

They did not have the on-prem Exchange problem, which they acknowledge is a big challenge at other universities.

k. What are the main advantages and limitations you've observed with using Keycloak (or alternative systems) for MFA?

They performed a POC (Proof of Concept) comparing Keycloak with "privacyIDEA". Ultimately, they chose Keycloak due to existing customizations, developer familiarity, and stronger out-of-the-box support for WebAuthn.

Limitations include that, if you need hardware tokens like RSA with 6-digit codes, you might have to configure or develop additional plugins.

l. How do you balance security and usability from a technical standpoint?

They prioritize multiple MFA methods so users can pick what suits them best, allowing a broad range of second-factor options so nobody feels forced to install a single official app on their phone. Also, they allow "device trust," so repeated logins on the same device require fewer second-factor prompts.

m. Are there any improvements or changes planned for the current MFA system at your university?

They might eventually explore passwordless authentication (FIDO2, WebAuthn).

Besides, not all applications were integrated on day one, so they plan to migrate a few remaining services to Keycloak.

Longer-term changes could arise if they adopt M365 or a new groupware solution, but that's an ongoing discussion.

n. What ideas or best practices from your experience do you think could be relevant or adaptable for other universities considering a similar path?

If on-prem Exchange is involved, you might need additional bridging solutions or to re-evaluate that environment.

Interview 4: Austrian University B - Technical Portfolio Manager

a. Do you use mandatory MFA at your University?

Yes, partially. Currently, mandatory MFA is enforced for staff only. Starting next spring, next steps towards mandatory MFA for students will be taken — once an agreement with the student union (ÖH) is reached.

b. What were the initial motivations for implementing it?

Strengthening security posture (Bring Your Own Device, new tech trends, eIDAS compliance, etc.), handling large-scale authentication demands (100k+ users), and preparing for the future of identity, including potential biometric factors, ID Austria, eIDs for international students, etc.

c. What organizational strategies were employed to roll out MFA smoothly?

For students, the plan is to have a gradual rollout, potentially targeting specific cohorts or faculties first. They must coordinate with the ÖH (student union) and provide user-centered experiences (accessible, inclusive). Also, the interviewee emphasizes the importance of user experience: Technology should stay "in the background," with minimal user friction.

d. What communication strategies are most effective in gaining acceptance by students and staff?

The interviewee believes that for a large, diverse population (including older learners, disabled users, etc.), user-centered communication is crucial. Besides, short, low-threshold instructional videos can be provided (no massive workshops because the user base is huge).

Furthermore, a successful transformation requires clear and inclusive messaging that addresses accessibility (WZAG (Web-Zugänglichkeits-Gesetz) compliance), and a sense of why MFA is needed.

e. How is the decision to implement mandatory MFA met? Are the students involved in this decision?

The process for students is "authoritative"—the university decides, and the student union (ÖH) is informed. However, the interviewee acknowledges that a more participatory approach would be ideal, but reality is that the university (and the Rektorat) is making top-down decisions. In addition, the interviewee also underlines the importance of universities cooperating in these matters.

f. How do students and staff respond to mandatory MFA? Were there significant changes in user experience?

For staff, mandatory MFA is already in place; no major user feedback is mentioned. For students, it has not rolled out yet, so there is no direct acceptance data. The interviewee predicts some pushback (from around 15% of students at first) but believes most will adapt if communication is handled well.

g. Are there any specific incentives that improve user compliance? How did/will you handle resistance?

The speaker highlights the importance of change management. In their experience, the most successful projects involve more people working on change management than on project management, especially in digital transformation projects.

h. Do you think a phased/gradual approach is necessary for success (for a smooth transition to mandatory MFA)?

Yes, they favor gradual rollouts, especially for a student population of 100k+. They plan to test with certain user groups or faculties first before scaling up. Starting with master students could be beneficial, as they are already accustomed to everyday student life.

i. Could you very briefly describe the current state of identity management and authentication mechanisms at your university?

Basically, there two systems that use MFA: Microsoft 365 with Entra ID and MFA, plus an F5-based VPN requiring MFA. The university uses Shibboleth (SAML) for many internal web-based services, but it is considering how to integrate or possibly replace that with more modern solutions. For identity management, they use One Identity via the BRZ. They have a central IdP integrated with the ACOnet federation.

The speaker believes in eventually moving to more standard or cloud-based MFA solutions rather than custom approaches. On the other hand, they still try to avoid vendor lock-in as far as possible. More detailed information cannot be disclosed due to security reasons.

j. How do you balance security and usability from a technical standpoint?

The main priority is user-centered design: minimal friction for large, diverse populations. They mention the difficulty of requiring personal phones vs. giving out hardware tokens (which can be “yesterday’s tech”). Besides, they anticipate a shift to passkeys, biometrics, or other low-friction methods soon.

k. Were there any specific measures taken to minimize the invasiveness of MFA (e.g., using context-based authentication)? How strict is your MFA implementation?

The current MFA usage is relatively standard (e.g., Microsoft Hello, Microsoft Authenticator). They have not yet implemented advanced context-based rules for the entire user base.

l. Are there any improvements or changes planned for the future?

They plan a major student rollout in 2025.

For the future, they are looking at next-gen authentication: passkeys, biometric methods, "Bring Your Own Identity" concepts, integration with eIDAS, ID Austria, etc. They note that advanced "continuous authentication", "AI-driven" verification and Self-Sovereign Identities might be on the horizon, though not imminent.

They also see potential for shared services with other universities (e.g., ACOnet), but that requires universities to unify their policies.

m. What key lessons did you learn from the rollout of MFA that could benefit other institutions?

Emphasize a user-centered approach—don't treat MFA as purely technical. Consider inclusivity (age, disability, etc.).

Communicate the "why" behind MFA and address privacy concerns (especially at universities with strong data-protection sentiment).

Policy consistency: The biggest challenge is to ensure the university leadership enforces the policy uniformly, without exceptions for vocal professors or departments.

Particularly for TU Wien: The speaker suggests that if on-prem Exchange is a major blocker, one might consider migrating to an alternative system (e.g., Open-Xchange) or a different approach.

n. Additional question: What do you see as the main differences between implementing MFA at a university compared to a commercial (private-sector) organization?

Universities have a strong culture of **academic freedom**, which often means more resistance to mandatory security measures. In commercial settings, it's more common for senior management to simply mandate MFA without the same level of pushback. A commercial firm often adopts a top-down approach (mandate from leadership). Academic institutions typically need broader consensus (involving student unions and faculty committees) to gain acceptance for any major change.

At many universities, **policy enforcement** is relatively weak: If a prominent professor or department complains, decisions can get overturned or watered down. In companies, a top-level executive (e.g., CIO) can typically enforce security policies more consistently across the whole organization.

Universities may have **limited staff** (FTEs) to manage complex MFA rollouts, yet they can serve massive user populations (e.g., 100k+ students).

In higher ed, **user demographics** range from "digital natives" to older students (some are 90+), plus staff with widely varying tech skills. This demands inclusive and accessible MFA solutions.

Universities rely heavily on Bring Your Own Device (**BYOD**). Most students/staff do not receive standardized hardware from the institution. Requiring personal

phones for MFA can introduce privacy or cost concerns. Many companies provide corporate devices, making MFA enrollment smoother.

Interview 5: Austrian University B - DevOps Engineer

a. Do you use mandatory MFA at your University?

There is some form of MFA at university B, especially for VPN access. For staff (personnel) who use Microsoft 365, MFA is mandatory. Students who choose to use the VPN also must enable MFA, but it is not (yet) enforced across all other student services.

b. What organizational strategies are (going to be) employed to roll out MFA smoothly?

The first phase was to enable MFA for staff, which could be seen as a first testing phase group of 10k-20k people. Next, gradually, all services will have to migrated to a single IAM solution (Keycloak) step by step. Finally, once this migration is complete and a comprehensive rollout of mandatory MFA would be feasible, the interviewee suggests that MFA can be enabled for all students simultaneously.

The interviewee adds that a large scale rollout to all students needs to be announced at least three months prior to the target date. This is necessary for students that e.g., do not have smartphones and therefore need to be equipped with YubiKeys or any other authentication devices.

c. What communication strategies are most effective in gaining acceptance by students and staff?

The interviewee mentions the user perspective for the current state of MFA rollout: Staff "realize they need VPN for home office," so they comply with MFA. Students use it far less, so acceptance is not strongly tested.

d. How do students and staff respond to mandatory MFA? Are there significant changes in user experience?

Staff: They mostly accept it because they need VPN for home office, so it is "almost no alternative."

Students: Only a small subset uses VPN (e.g., printing from home), so the MFA requirement is minimal for them.

The interviewee notes that for typical student activities (Moodle, etc.), MFA is not currently mandated, so widespread adoption or pushback is not really happening.

e. Could you very briefly describe the current state of identity management and authentication mechanisms at your university?

In addition to the current MFA implementation for staff (especially via VPN), the university uses Shibboleth (SAML) for single sign-on in many cases, but it does not always offer a fully seamless experience.

f. Does your university use Keycloak as part of your identity and access management system? If so, what role does it play in this system? If not, what other solutions are in place?

Currently, Keycloak is not the main MFA solution for VPN. Shibboleth is more established. However, the interviewee mentions the university's future plan to adopt it more broadly for SSO. The university wants to bring "most services" under Keycloak for centralized authentication. They note that they have "many different login masks" right now, and unifying them via Keycloak is part of a broader strategy.

g. What are the main advantages and limitations you've observed with using Keycloak for MFA?

Advantages: A strong community exists around Keycloak, meaning plenty of resources. Once properly configured, Keycloak generally "just works" as intended, saving time later on.

Limitations: Certain features require customization, it won't work "out-of-the-box".

h. How configurable and scalable have you found Keycloak to be, especially when it comes to integrating it with legacy systems?

Unlike TU Wien, this university does not have on-prem Exchange for students. No Exchange-based mail accounts for students means fewer integration hurdles with Keycloak (no "Exchange + Keycloak" mismatch).

i. How do you balance security and usability from a technical standpoint?

The speaker is aware that MFA can be "annoying" for repeated logins. They emphasize that a strong Single Sign-On approach is crucial to reduce friction. If you only log in once (even with MFA), it is much more bearable than repeated factor prompts.

j. Are there any improvements or changes planned for the current MFA system at your university?

The interviewee suggests that eventually MFA might be required for more student services (Moodle, etc.).

They mention that the university is considering broader adoption of **Keycloak**, but no firm date or plan is given.

They want to adopt **ID Austria** to reduce friction in the future: They note that many younger users (e.g., new high school graduates) already have ID Austria set up. By leveraging ID Austria, the university can reduce the overhead of managing a separate MFA infrastructure (since ID Austria is already a "two-factor" system).

Furthermore, Passkeys might also be considered a future possibility for more passwordless logins. The speaker mentions concerns about vendor hosting (e.g.,

large American tech companies controlling passkey storage). Still, passkeys are on their radar as a more user-friendly authentication method down the road (definitely not in 2025 though).

3.3 Evaluation & Summary

In this section, first the internal and external interviews are summarized and compared. Afterwards, the gathered insights are linked to the research questions, effectively answering them.

3.3.1 Internal Interviews

The following knowledge base for the current situation at TU Wien has been established:

TU Wien is currently working on adapting its Identity and Access Management. The focus is on implementing MFA and consolidating existing authentication methods. TU Wien's goal/motivation is to ensure digital sovereignty and avoid dependence on large vendors.

Currently, there are two central authentication hubs:

- Single Sign-On (SAML): Central Identity Provider for the main TU account, covering main student platforms. This is aligned with the ACOnet Federation.
- Active Directory (AD) / LDAP: Mainly used for on-premise services like Microsoft Exchange and Teams.

In theory, all authentication processes—apart from Microsoft Exchange—could be migrated to the SSO solution. However, Exchange poses a challenge, as it cannot simply be integrated into an SSO infrastructure (e.g., Keycloak). Consequently, a complete consolidation into a single solution is not technically feasible, which is why alternative approaches are being explored.

An important step toward MFA that has already been implemented was the introduction of geofencing to restrict MFA access via VPN from outside the EEA. In addition, the product NetIQ is being evaluated as a potential central IAM solution. Alternatives such as Cisco Duo are also under consideration, with the aim of minimizing dependencies on proprietary solutions.

In theory, a switch from M365 to openDesk or Open-Xchange would also be conceivable (though it was only briefly mentioned), but it would likely be difficult to implement and might face resistance from students.

When it comes to future MFA integration/rollout strategies, both interviewees strongly indicated that a phased or iterative rollout is more realistic than a "big bang". They stressed that TU Wien's environment is too fragmented (SSO vs. AD/Exchange) for an immediate switch. Also, for better user acceptance, gradual onboarding can avoid overwhelming staff and students.

Furthermore, when balancing security and usability, both interviews showed a clear preference for strenghtening SSO, since requiring too many multiple MFA prompts likely frustrates students. The goal is to centralize as many services as possible under one login flow.

3.3.2 External Interviews

First, the current state of MFA, including the technical and organizational approach, of both external Austrian universities are summarized separately. Then, similarities and differences are discussed.

Summary MFA at Austrian University A

- **Current State of MFA:** The university A implemented MFA as a mandatory requirement for all users (staff and students) by early 2024. The process included an initial voluntary phase followed by a short “nag-screen” period, after which MFA became fully enforced. The university reports high coverage of second-factor registration, minimal pushback after the nag-screen period, and smooth integration without major compatibility problems (no on-prem Exchange for students).
- **Technology and Keycloak:** The university A relies on Keycloak for single sign-on (SSO) and MFA. This solution supports multiple authentication methods (TOTP apps, FIDO/WebAuthn, Windows Hello, etc.), providing users with flexibility when choosing their second factor.
- **Implementation Strategy:**

  The decision to rollout mandatory MFA was met top-down.

  MFA was rolled out using a phased approach. Voluntary adoption allowed the IT support team to gather feedback and address issues.

  A two-week grace period using a "nag screen" prompted users to set up MFA before being locked out.

  In order to communicate the MFA introduction effectively, short tutorial videos, documentation and early involvement with student union (ÖH) helped to minimize disruption.

Summary MFA at Austrian University B

- **Current State of MFA:** Mandatory MFA is enabled for staff, for students it is planned: University employees who need remote access or certain services (e.g., Microsoft 365, VPN) are already required to use MFA. While students need to enable MFA for VPN, it is not yet mandated across all services (e.g., Moodle). The university intends to expand coverage in the future.

- **Technology and Keycloak:** Keycloak is envisioned as a unifying IAM solution. The goal is to consolidate various login paths, which are currently split between AD, SAML IdPs, and isolated services, into one central system.
  The University also plans to adapt ID Austria for their logins. Most Austrian high school graduates already have ID Austria set up, plus, ID Austria is already a two-factor system.

- **Implementation Strategy:**

  The decision to rollout mandatory MFA was met top-down.

  The process to achieve mandatory MFA for all users will be a mixture of phased and larger big bang approaches. The first phase was to implement MFA for VPN and staff. Next phases will focus on the migration of most services toward Keycloak. Finally, once the infrastructure and policies are ready, mandatory MFA can be enabled for all students at once (i.e., "big bang"). They try to not allow for individual departments stalling or suspending the MFA rollout.

  University B emphasizes user acceptance. They aim to ensure single sign-on sessions remain active for a reasonable time, minimizing repeated prompts. Students and decentralized departments require clear guidelines to avoid confusion.

Similarities between the Universities

1. Both institutions view Keycloak as a core component for MFA.
2. Neither university A nor university B uses on-prem Exchange for student email, thereby avoiding one of the more challenging integrations with on-prem Microsoft systems and e.g., Keycloak.
3. Both have rejected an immediate "big bang" approach. Instead, they rely on staged rollouts and communication to build user acceptance. However, the university B still considers rolling out MFA for all students simultaneously, once ready.
4. To limit user frustration, both universities aim to provide single sign-on sessions and multiple second-factor options. Both recognize that MFA introduces extra steps that need to be balanced from both security and usability perspectives.
5. Both universities participate in the ACOnet federation.
6. They also show interest in passkeys for a more passwordless environment in the future.

Differences between the Universities

While university A already enforces MFA for all users, university B only has coverage for staff and partial coverage for students. The timeline for full student coverage remains open for the latter university.

At the time of the interviews, University B considers ID Austria a promising way to offload second-factor management. And in general, University A tends to focus slightly more on hosting services strictly on-premise and avoid vendor lock-in.

3.3.3 Linking Results to Research Questions

In this last section of the semi-structured interviews methodology, the gathered insights are related to the three research questions:

What technical and user acceptance challenges must be considered when implementing a unified MFA system in an academic environment, and how do these challenges differ from those in other types of organizations?

Implementing a unified MFA setup in an academic environment involves coping with technical fragmentation (multiple authentication sources, on-prem vs. cloud apps) and a diverse user base with a strong culture of academic freedom. The users, mostly students, often view additional login steps as intrusive. Unlike in many commercial contexts with strong top-down cultures, universities deal with more autonomous faculties and a large, changing student population. Influential faculties or professors may limit policy enforcement by delaying or disapproving MFA decisions. Moreover, staffing constraints force usually rather small IT teams to serve very large user populations (sometimes over 100,000 students). These users range from “digital natives” to older, non-technical learners, necessitating inclusive, accessible solutions. Finally, universities rely heavily on Bring Your Own Device (BYOD). Most students do not receive standardized hardware from the institution. Requiring personal phones for MFA can introduce privacy or cost concerns. Many companies provide corporate devices, making MFA enrollment smoother.

How can MFA systems be tailored to meet the specific needs and constraints of higher-education environments while ensuring high user adoption?

Offering multiple additional-/second-factor methods for students to choose from, as well as providing a coherent single sign-on experience are required to maximize user adoption while meeting security needs. A university’s diverse user base requires user-friendly solutions that let each user choose tokens/keys, authenticator apps, or even passwordless options. From an organizational perspective, proactive engagement with stakeholder groups (e.g., student unions) and clear communication with students (most important: "WHY is MFA needed?") fosters acceptance.

What role can Keycloak, an open-source identity and access management solution, play in the architecture of a robust MFA system designed for educational environments?

By consolidating different login systems into a single identity and access management solution, Keycloak can lower operational overhead and simplify MFA enforcement across a wide range of campus services. Its support for modern authentication protocols (SAML, OIDC) and various MFA methods (e.g., TOTP, FIDO/WebAuthn), as well as wide customization possibilities, helps universities integrate their diverse identity services. However, for universities that host on-prem Exchange (as noted by internal interviews at TU Wien), integration with Keycloak remains a major limitation: Microsoft's on-prem mail server offers no straightforward path for external SSO or multi-factor integration. This forces institutions to maintain separate authentication methods or adopt vendor-specific workarounds (e.g., moving to the cloud).

CHAPTER 4

Framework Analysis

Based on the findings from the research phases from the SLR and the SSIs, a strategy for implementing a unified MFA solution is created. This involves designing a system architecture on a conceptual level and discussing its integration and deployment in academic environments.

In particular, this methodological step follows the framework analysis method, which is suited for systematically analyzing data to develop a strategy of a conceptual model, i.e., a framework [ST08]. It is a five steps method that encompasses familiarization with the data (from the literature review and expert interviews), developing a thematic framework that captures the identified key issues, indexing (or labeling) data to correspond to the themes of the framework, charting to visualize the summarized and indexed data and, finally, interpretation of the charted data to gather insights and inform the development of the conceptual prototype. Goldsmith [Gol21] further elaborates on these 5 steps, claiming that framework analysis is especially useful for applied qualitative research.

Disclaimer: The framework analysis used for this thesis does not explicitly include the charting/visualization of the indexed data, i.e., the fourth step is skipped. Since each finding is already indexed with its data source (either "SLR" or "SSI"), additional tables (charting) would not enhance the clarity or add further insight to the organization of the data. The current list format under the section Indexing: Mapping Findings to Themes shows the distribution and thematic categorization, rendering further tabular organization or visualization redundant. By adding the data source to the index, the charting is practically already included with the indexing step.

4.1 Familiarization with the Data

Both the literature review and the interviews highlight several common challenges and opportunities. The following is a brief summary of these commonalities:

4.1.1 Technical Fragmentation

Usually, within academic institutions multiple authentication backends exist, which complicate a unified approach. E.g., SSO is provided via OAuth, SAML, AD/LDAP and legacy systems such as on-prem Exchange. While solutions like Keycloak offer centralized identity mangement, their integration with certain legacy systems (e.g., on-prem Exchange) often remains problematic.

4.1.2 User Acceptance and Adoption

Mandatory MFA can lead to user frustration or security fatigue, particularly in a diverse academic environment. Both the literature and interviews underscore the importance of phased rollouts, user education, and proper communication to achieve high adoption.

4.1.3 Choice of MFA Methods and Flexibility

Providing multiple second-factor options (e.g., TOTP, WebAuthn, and emerging passwordless methods) increases user acceptance. Flexibility is key for accommodating various user groups and for mitigating the burden of repeated authentication prompts. This is especially important for academic environments where users range from digital natives to less tech-savvy staff and students.

4.1.4 Scalability and Vendor Independence

Adopting an open-source solution like Keycloak can reduce the dependency on proprietary vendors. On the other hand, scalability challenges and system-specific limitations of on-premise solutions need to be addressed.

4.2 Assessing the Core Themes

Based on these summarized insights, the developed thematic framework contains the following core themes:

- Integration & Technical Consolidation
- User-Centric Adoption
- MFA Method Diversity
- Change Management & Communication
- Scalability & Vendor Independence

4.3 Indexing: Mapping Findings to Themes

The findings from the systematic literature review and semi-structured interviews can be categorized under one or more of the themes. For the indexing, findings have been named "SLRX" and "SSIX" for the literature review and interviews respectively, where X is a running number.

4.3.1 Integration & Technical Consolidation

This first theme focuses on the consolidation of services and applications and centralization of identity and access management in academic institutions. As universities increasingly rely on multi-factor authentication to meet evolving security demands, the challenge lies in integrating fragmented authentication systems. In total, 20 findings were mapped to this theme and are listed below.

- SLR1: There is an increasing reliance on MFA to meet rising security needs.
- SLR3: Implementation examples from institutions (e.g., Kyushu University, Tokyo University of Agriculture and Technology) indicate that flexible MFA systems with user-driven enrollment are preferred.
- SLR5: There is a lack of comprehensive research on practical challenges and cost-effective strategies for integrating decentralized identity (blockchain/SSI) with existing academic systems.
- SLR6: There is an absence of a unified, widely adoptable framework for MFA implementation tailored to higher education institutions.
- SLR11: Keycloak is recognized as a highly flexible and adaptable open-source identity and access management solution.
- SLR12: Keycloak effectively supports centralized MFA, SSO, and identity management through industry-standard protocols (OAuth 2.0, OpenID Connect, SAML).
- SLR13: Keycloak is praised for its centralized session management and role-based access control, benefiting diverse academic environments.
- SLR14: Keycloak offers flexible configuration for MFA, including context-based authentication and integration with authenticator apps.
- SLR15: Successful deployments often require gradual migration strategies, including self-service tools for enrollment and smooth transition from legacy systems.
- SSI1: TU Wien is adapting its Identity and Access Management with a focus on implementing MFA and consolidating existing authentication methods to ensure digital sovereignty and avoid dependence on large vendors.

- SSI2: At TU Wien, two central authentication hubs are in place: a Single Sign-On (SAML) system for TUaccounts (covering systems like TISS, TUWEL, and Colab) and an Active Directory (AD)/LDAP system for on-premise services such as Microsoft Exchange and Teams.
- SSI3: Microsoft Exchange poses a significant integration challenge as it cannot be easily migrated to the SSO solution, making complete consolidation into a single system difficult.
- SSI4: At TU Wien, Geofencing has been introduced to restrict MFA access via VPN from outside the EEA, serving as an important security measure.
- SSI6: At TU Wien, a switch from M365 to alternatives like openDesk or Open-Xchange is being considered, though it is anticipated to face resistance from students.
- SSI8: At TU Wien, there is a clear preference for strengthening SSO to balance security and usability, thereby reducing the frustration caused by multiple MFA prompts and centralizing the login process.
- SSI10: Austrian University A relies on Keycloak for SSO and MFA, leveraging its support for multiple authentication methods (e.g., TOTP apps, FIDO/WebAuthn, Windows Hello) to offer flexibility for users.
- SSI12: At Austrian University B, mandatory MFA is currently enabled for staff, with plans to extend it to students. Currently, MFA is enforced for VPN access for students, while other services are not yet covered.
- SSI13: Austrian University B envisions Keycloak as a unifying IAM solution that consolidates diverse login paths—currently split among AD, SAML IdPs, and isolated services—and plans to integrate ID Austria for user logins.
- SSI16: Similarities between the Austrian Universities A and B include viewing Keycloak as central to MFA, avoiding on-prem Exchange for student email.
- SSI22: The prevalent BYOD culture in academia introduces additional privacy and cost challenges for MFA enrollment, contrasting with commercial environments where standardized devices are more common.

4.3.2 User-Centric Adoption

This theme examines the role of user experience in a multi-factor authentication adoption. As mandatory MFA can lead to frustration, universities must balance security requirements with user convenience. Findings highlight the importance of phased rollouts, user-driven enrollment, and flexible authentication methods. In total, 12 findings were mapped to this theme and are listed below.

- SLR3: Implementation examples from institutions (e.g., Kyushu University, Tokyo University of Agriculture and Technology) indicate that flexible MFA systems with user-driven enrollment are preferred.
- SLR4: Gradual transitions are necessary, as immediate, mandatory MFA enforcement tends to face significant user resistance.
- SLR15: Successful deployments often require gradual migration strategies, including self-service tools for enrollment and smooth transition from legacy systems.
- SLR18: MFA can impose significant user experience challenges, such as frustration, stress, and security fatigue when enforced universally.
- SLR19: Users generally prefer MFA only for highly sensitive systems rather than for every login.
- SLR20: Balancing security with usability is essential; voluntary opt-ins or context-based exemptions can lead to a more positive user experience.
- SSI6: At TU Wien, a switch from M365 to alternatives like openDesk or Open-Xchange is being considered, though it is anticipated to face resistance from students.
- SSI7: At TU Wien, both interviewees recommend a phased or iterative rollout for future MFA integration rather than a “big bang” approach, citing the fragmented environment (SSO vs. AD/Exchange) and the need to avoid overwhelming staff and students.
- SSI8: At TU Wien, there is a clear preference for strengthening SSO to balance security and usability, thereby reducing the frustration caused by multiple MFA prompts and centralizing the login process.
- SSI9: Austrian University A implemented mandatory MFA for all users (staff and students) by early 2024, following an initial voluntary phase and a subsequent “nag-screen” period that enforced MFA setup.
- SSI11: The implementation strategy at Austrian University A involved a top-down decision, a phased rollout, and extensive communication measures—including tutorial videos, documentation, and early engagement with the student union—to facilitate smooth user adoption.

- SSI15: Both Austrian Universities A and B aim to provide extended single sign-on sessions and multiple second-factor options to minimize user frustration, and they express interest in adopting passkeys for a more passwordless environment in the future.

4.3.3 MFA Method Diversity

This theme explores the evolving landscape of authentication methods. It highlights a shift towards diverse and passwordless MFA approaches. The findings below emphasize the need for further research into emerging methods, the flexibility of modern IAM solutions, and the importance of offering multiple authentication options. In total, 11 findings were mapped to this theme and are listed below.

- SLR2: There is an emergence of new identity management methods, such as biometrics and blockchain-based solutions (self-sovereign identities).
- SLR5: There is a lack of comprehensive research on practical challenges and cost-effective strategies for integrating decentralized identity (blockchain/SSI) with existing academic systems.
- SLR7: In general (not specific to academic environments), there is a notable shift toward multi-factor and passwordless authentication methods to overcome the limitations of single-factor authentication.
- SLR8: Modern authentication methods include biometrics, public key infrastructure certificates, FIDO2 keys, continuous authentication, adaptive authentication, and graphical passwords.
- SLR9: There is only limited research on the feasibility and practical readiness of certain authentication methods, especially graphical passwords.
- SLR10: More evidence is needed to assess the usability and robustness of continuous and adaptive authentication methods in real-world scenarios.
- SLR14: Keycloak offers flexible configuration for MFA, including context-based authentication and integration with authenticator apps.
- SSI4: At TU Wien, Geofencing has been introduced to restrict MFA access via VPN from outside the EEA, serving as an important security measure.
- SSI10: Austrian University A relies on Keycloak for SSO and MFA, leveraging its support for multiple authentication methods (e.g., TOTP apps, FIDO/WebAuthn, Windows Hello) to offer flexibility for users.
- SSI13: Austrian University B envisions Keycloak as a unifying IAM solution that consolidates diverse login paths—currently split among AD, SAML IdPs, and isolated services—and plans to integrate ID Austria for user logins.

- SSI15: Both Austrian Universities A and B aim to provide extended single sign-on sessions and multiple second-factor options to minimize user frustration, and they express interest in adopting passkeys for a more passwordless environment in the future.

4.3.4 Change Management & Communication

This theme is concerned with the role of change management and communication in the successful implementation of mandatory multi-factor authentication. The findings below highlight best practices from universities and the importance of balancing security with usability. In total, 11 findings were mapped to this theme and are listed below.

- SLR4: Gradual transitions are necessary, as immediate, mandatory MFA enforcement tends to face significant user resistance.
- SLR20: Balancing security with usability is essential; voluntary opt-ins or context-based exemptions can lead to a more positive user experience.
- SLR21: Further research is needed to explore effective communication strategies that clearly demonstrate the benefits of MFA to end users.
- SSI7: At TU Wien, both interviewees recommend a phased or iterative rollout for future MFA integration rather than a "big bang" approach, citing the fragmented environment (SSO vs. AD/Exchange) and the need to avoid overwhelming staff and students.
- SSI9: Austrian University A implemented mandatory MFA for all users (staff and students) by early 2024, following an initial voluntary phase and a subsequent "nag-screen" period that enforced MFA setup.
- SSI11: The implementation strategy at Austrian University A involved a top-down decision, a phased rollout, and extensive communication measures—including tutorial videos, documentation, and early engagement with the student union—to facilitate smooth user adoption.
- SSI12: At Austrian University B, mandatory MFA is currently enabled for staff, with plans to extend it to students. Currently, MFA is enforced for VPN access for students, while other services are not yet covered.
- SSI14: The Austrian University B employs a mixed implementation strategy that starts with a phased rollout for VPN and staff, followed by a broader migration toward Keycloak, and ultimately a "big bang" approach for full student coverage once infrastructure and policies are ready.
- SSI17: Similarities between the Austrian Universities A and B include rejecting an immediate "big bang" approach in favor of staged rollouts, and emphasizing clear communication to foster user acceptance.

- SSI18: Universities face greater resistance to mandatory MFA due to a culture of academic freedom that requires broad consensus, unlike the top-down mandates typical in commercial organizations.
- SSI19: Policy enforcement in universities is often weak and subject to influence (e.g., from individual professors), whereas commercial organizations can enforce security policies more consistently through top-level management.

4.3.5 Scalability & Vendor Independence

The last theme addresses the scalability of identity and access management solutions and the importance of vendor independence and data ownership in academic institutions. In total, 8 findings were mapped to this theme and are listed below.

- SLR11: Keycloak is recognized as a highly flexible and adaptable open-source identity and access management solution.
- SLR13: Keycloak is praised for its centralized session management and role-based access control, benefiting diverse academic environments.
- SLR16: There is limited empirical research on Keycloak's scalability and performance in large-scale academic settings.
- SLR17: Best practices for securely configuring Keycloak's customizable elements (e.g., Service Provider Interfaces) remain underexplored.
- SSI1: TU Wien is adapting its Identity and Access Management with a focus on implementing MFA and consolidating existing authentication methods to ensure digital sovereignty and avoid dependence on large vendors.
- SSI5: At TU Wien, the evaluation of potential central IAM solutions like NetIQ is underway, with alternatives such as Cisco Duo being considered. However, considerations about minimizing the reliance on these proprietary solutions are ongoing.
- SSI13: Austrian University B envisions Keycloak as a unifying IAM solution that consolidates diverse login paths—currently split among AD, SAML IdPs, and isolated services—and plans to integrate ID Austria for user logins.
- SSI20: Limited IT staffing in universities, despite managing massive user populations, complicates the rollout and management of complex MFA systems.

4.4 Interpretation and Strategy

Based on the indexed data, the following strategy for implementing a unified MFA solution can be proposed:

4.4.1 Consolidate and Centralize Identity Management

In the realm of Integration & Technical Consolidation, the literature (SLR1, SLR3, SLR5, SLR6, SLR11, SLR12, SLR13, SLR14, SLR15) emphasizes the need for a centralized approach to address the rising security demands through MFA. In academic settings, one of the primary challenges is managing a wide variety of authentication systems that serve diverse applications. Interview data from TU Wien (SSI1, SSI2, SSI4, SSI6, SSI8) and external Austrian universities (SSI10, SSI12, SSI13, SSI16, SSI22) further confirm that consolidation via a unified IAM system can streamline authentication processes. This leads to a strategy focused on adopting an integrated IAM platform.

To address this, the first step is to consolidate and centralize authentication services using a platform such as Keycloak. This centralization enables universities to integrate diverse authentication methods — whether they rely on SAML-based single sign-on, AD/LDAP directories, or other legacy systems — into one cohesive framework. By unifying these systems under a single platform, academic institutions can streamline administrative tasks, enforce consistent security policies, and support modern protocols such as OAuth 2.0 and OpenID Connect. Nonetheless, as described with SSI3 and SSI16, it is important to recognize that some legacy systems, especially those that do not natively support modern MFA integration, may require additional bridging solutions or a gradual phase-out in favor of more compatible alternatives.

4.4.2 Implement an Iterative Rollout Strategy

The collective data clearly advocate for an iterative, phased implementation of MFA rather than an immediate, all-encompassing rollout. Findings from the literature (SLR4, SLR15, SLR18, SLR20) reveal that mandatory, immediate MFA enforcement can lead to user frustration and resistance, especially in academic settings where user populations are diverse and subject to rapid change. This is further supported by interview insights (SSI7, SSI9, SSI11, SSI12, SSI14) from both TU Wien and other universities, which stress that gradual adoption — starting with a voluntary phase supported by clear communication and a “nag-screen” period — is more effective.

Universities should begin with pilot projects in less critical areas to test the new MFA system in a controlled setting. This phased approach allows IT teams to gather real-world feedback, address unforeseen integration challenges, and make necessary adjustments before extending the solution institution-wide. Over time, as confidence in the system grows and technical issues are resolved, the solution can then be deployed more broadly. One way to do this would be to iteratively integrate service after service to a central IAM solution.

4.4.3 Enhance User Adoption Through Communication and Training

The indexed findings underscore the importance of user acceptance for a successful implementation of MFA in academic environments. Literature (SLR3, SLR4, SLR15, SLR18, SLR19, SLR20) reveals that while flexible, user-driven enrollment is preferred. Abrupt or mandatory enforcement often leads to frustration, stress, and security fatigue. Interview data from TU Wien and other universities (SSI6, SSI7, SSI8, SSI9, SSI11, SSI15) again demonstrate that a phased, iterative approach is essential for achieving broad user adoption.

To foster acceptance, it is vital to develop a comprehensive communication strategy that clearly explains the benefits and necessity of MFA. Institutions should create accessible instructional materials such as short explainer videos, detailed step-by-step guides, and easy-to-understand FAQs that justify the MFA process. Furthermore, early engagement with various stakeholders such as student unions and faculty representatives is also essential. These efforts help ensure that users understand not only how to use the system but also why it is necessary for enhancing overall security. Moreover, consistent training sessions and the availability of responsive IT support can improve overall user satisfaction and compliance.

4.4.4 Offer Multiple MFA Methods to Balance Security and Usability

As discovered by the literature review (SLR2, SLR7, SLR8), new identity management methods are emerging. A key insight from both the literature (SLR5, SLR9, SLR10, SLR14) and the interviews (SSI4, SSI10, SSI13, SSI15) is the importance of providing a variety of these authentication options to meet diverse user needs. Modern academic environments are increasingly adopting methods like TOTP, biometrics, WebAuthn, FIDO2 keys, and adaptive authentication techniques, that the students can choose from. This variety is critical to accommodate the different technical skills and preferences across the heterogeneous user base at universities. Finally, the finding SSI15 stresses the importance of solid and long SSO sessions to minimize user frustration.

4.4.5 Ensure Scalability and Discuss Vendor Independence

Scalability and vendor independence are essential considerations for long-term success in MFA implementation. It is crucial to ensure that the chosen MFA solution can scale effectively with the university's growing needs and to discuss any dependencies to any single vendors. The literature (SLR11 and SLR13) highlights that open-source platforms like Keycloak provide the necessary flexibility to adapt and extend the system over time, thereby reducing the risk of vendor lock-in. Interview findings (SSI1, SSI5, SSI13, SSI20) support this by noting that academic institutions, which are often constrained by limited IT staffing, yet responsible for managing large user populations, require solutions that can evolve and perform efficiently under increasing demand. The results of all interviewed universities show a tendency towards maintaining digital sovereignty, e.g., as opposed to moving to proprietary clouds.

CHAPTER 5

Practical Demonstration of Multi-Factor Authentication with Keycloak

To practically evaluate Keycloak's capabilities for multi-factor authentication, a small-scale prototype environment was established. The implementation of this prototype is supposed to serve as validation of the proposed strategy, providing concrete insights into its feasibility and integration within university IT environments.

In this chapter, first the prototype environment and the configuration of Keycloak is described. Afterwards, practical insights and experiences are shared, with a focus on implications for large academic institutions and references to the case study at TU Wien.

5.1 Overview of Prototype Environment

The setup was performed on a local development environment using Docker[1] on a 2020 Apple MacBook Air (M1)[2]. Using Docker, Keycloak's containerized distribution could be hosted without any further installation and prerequisites. For this purporse, the latest Keycloak container image from Red Hat's Quay.io was run[3]. At the time of testing, this latest version was Keycloak version 26.1.3.

In this environment, a dedicated Keycloak realm, test users, and Time-based One-Time Password (TOTP) as a second-factor authentication method were configured. To simulate

[1] Docker: `https://www.docker.com`. Accessed: 2025-03-05

[2] Apple MacBook Air (M1, 2020) - Technical Specifications: `https://support.apple.com/en-us/111883`. Accessed: 2025-03-05

[3] Keycloak container image on Quay.io: `https://quay.io/repository/keycloak/keycloak`. Accessed: 2025-03-05

application integration, a hypothetical client application was registered in Keycloak, using OpenID Connect. This minimal environment demonstrates Keycloak's functionality and allows for consideration about how to integrate existing applications and authentication infrastructures.

5.2 Configuration of Keycloak

After launching a Keycloak server on port 8080 of localhost using the Docker image, and logging in using the provided admin credentials, the user is presented with the default master realm, as can be seen in the screenshot below (Figure 5.1).

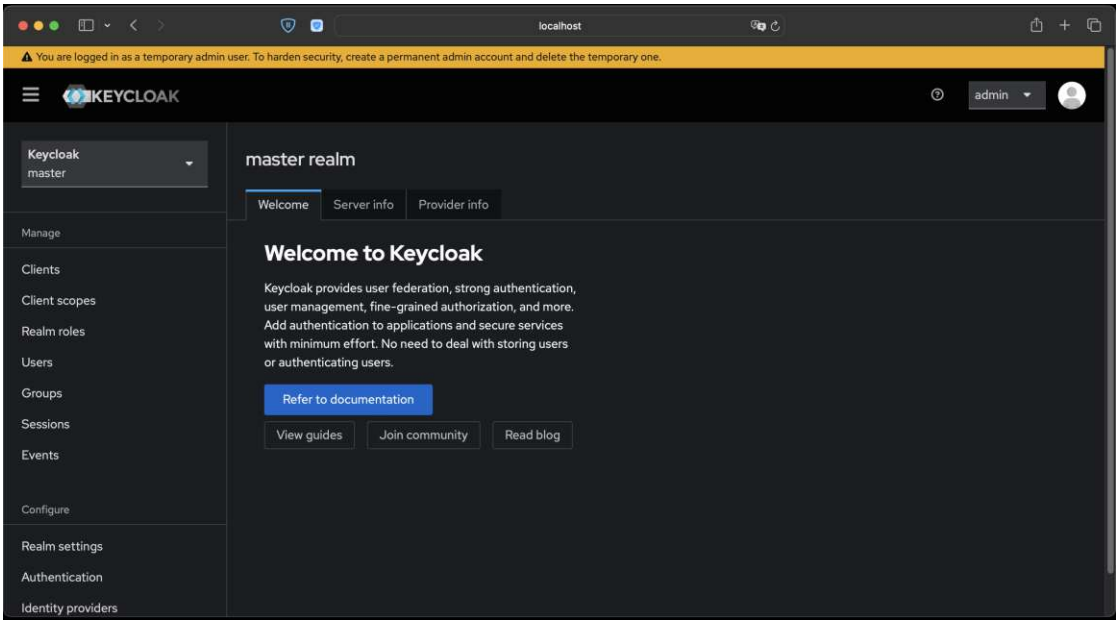


Figure 5.1: Default master realm after launching Keycloak server.

As the first configuration step, a new Keycloak realm ("TUWienDemoRealm") was configured to simulate a university environment. As explained in Figure 5.2, a realm manages a set of users, credentials, roles and groups, isolating authentication and control over users. A potential use case for this would be the enablement of proper application lifecycle management (ALM) by providing different realms for the separation of development, testing and production environments.

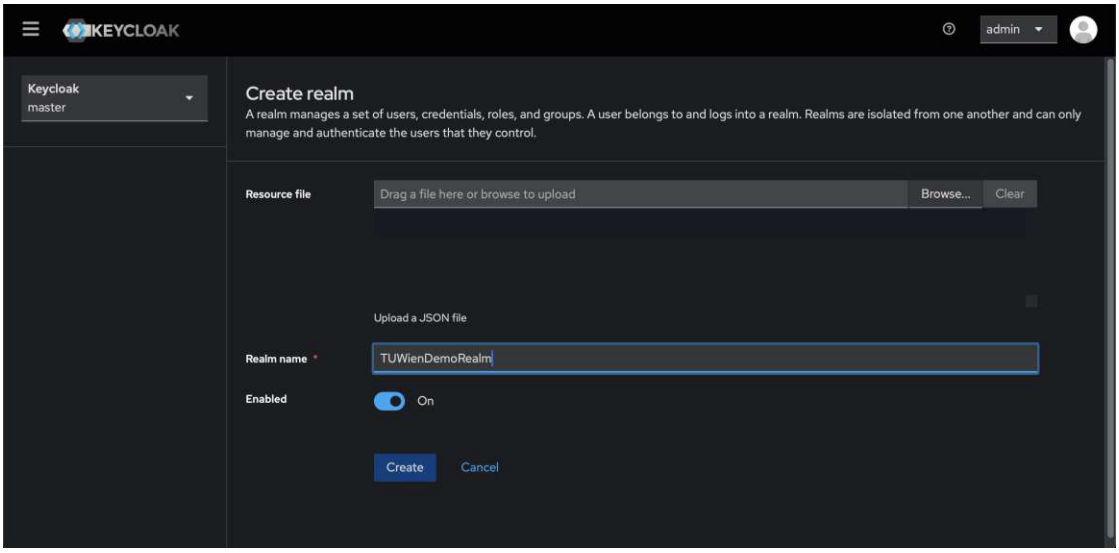


Figure 5.2: Creation of a demo realm to simulate an academic environment.

Next, in the newly created demo realm, groups were created to facilitate the management of roles and attributes for future adaptations of the setup. Useful examples for groups in the context of academic environments would be faculties or even individual study programmes. For the sample demo, two simple groups for staff and students were created, as pictured in Figure 5.3.

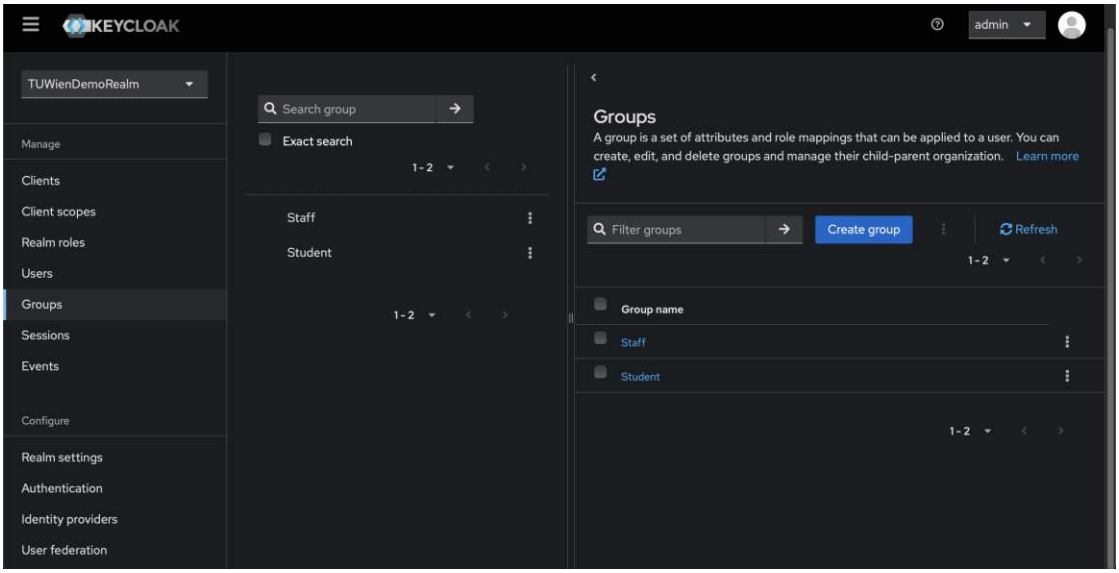


Figure 5.3: Creation of groups for students and staff.

Afterwards, the first user was created and assigned to the new group for students. For this purpose, only the username was set (Figure 5.4). By default, the user will have to

set the email address, first-name and last-name upon logging in for the first time, if these fields are not initialized when creating the user. Furthermore, by selecting "Configure OTP" under the required user actions, the user will be prompted to setup an additional OTP factor with a mobile authenticator app.

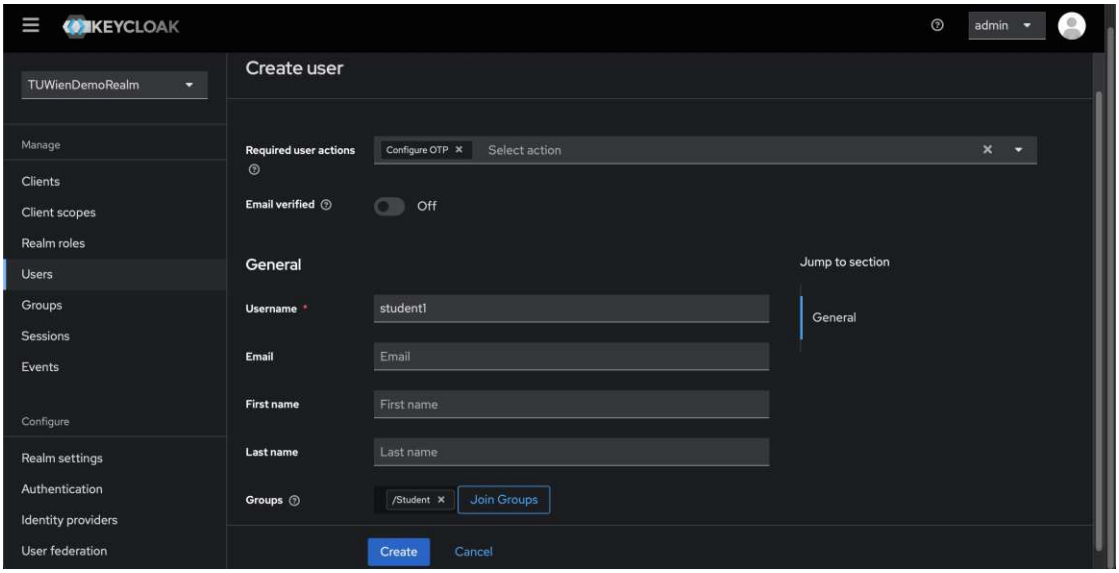


Figure 5.4: Creation of a user for a student.

Instead of individually assigning the required user actions, OTP can also be activated by default for all new users:

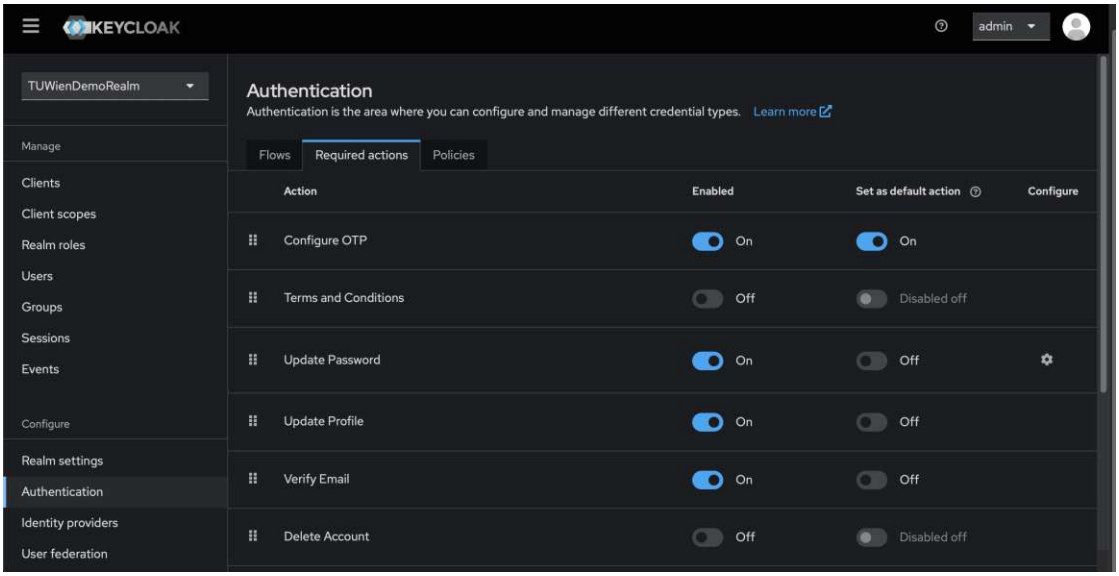
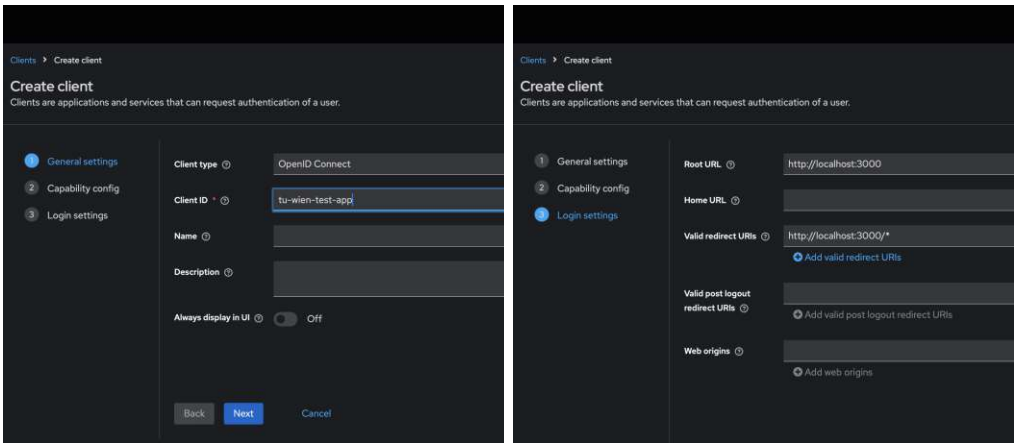


Figure 5.5: Enabling OTP as required action for authentication.

In the last step of the initial setup, a sample client application was registered (Figure 5.6. Client applications and services can then use Keycloak to authenticate their users. For the creation of the hypothetical client application the protocol OpenID Connect was selected, and the root URL of the application as well as allowed redirect URIs the client application can use were defined.



(a) General settings. (b) Login settings.

Figure 5.6: Creation of a sample client application.

After this initial setup, in order to test this MFA configuration, we first set a temporary password for the user "student1". As shown in Figure 5.7, by enabling "Temporary" when setting the password, the user will be forced to change the password when logging in the next/first time.

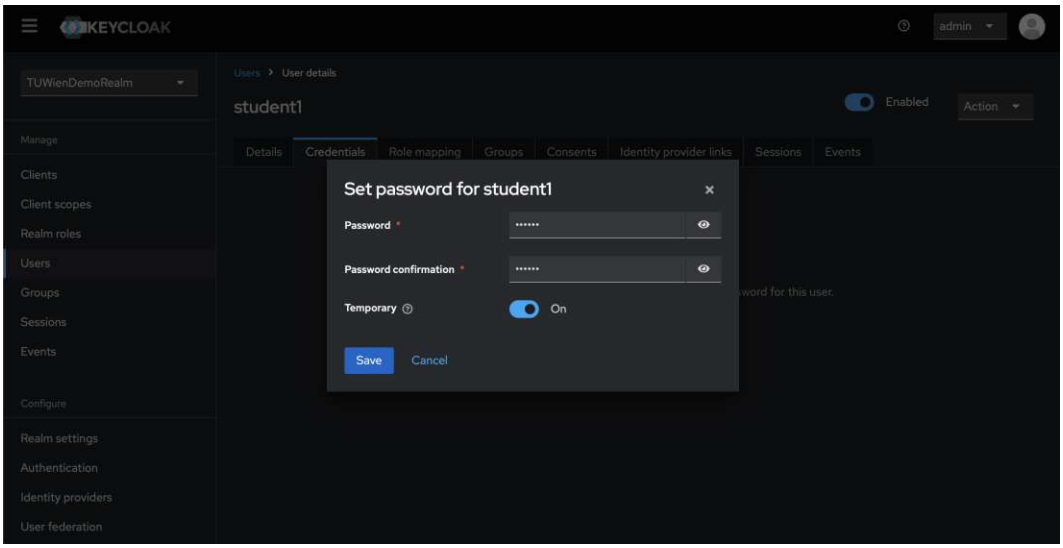


Figure 5.7: Setting a temporary password for the test user.

As the created sample client "tu-wien-test-app" is purely hypothetical, i.e., there is no application running on port 3000 of the localhost, the automatically created "account-console" for this demo realm was used to demonstrate the MFA setup.

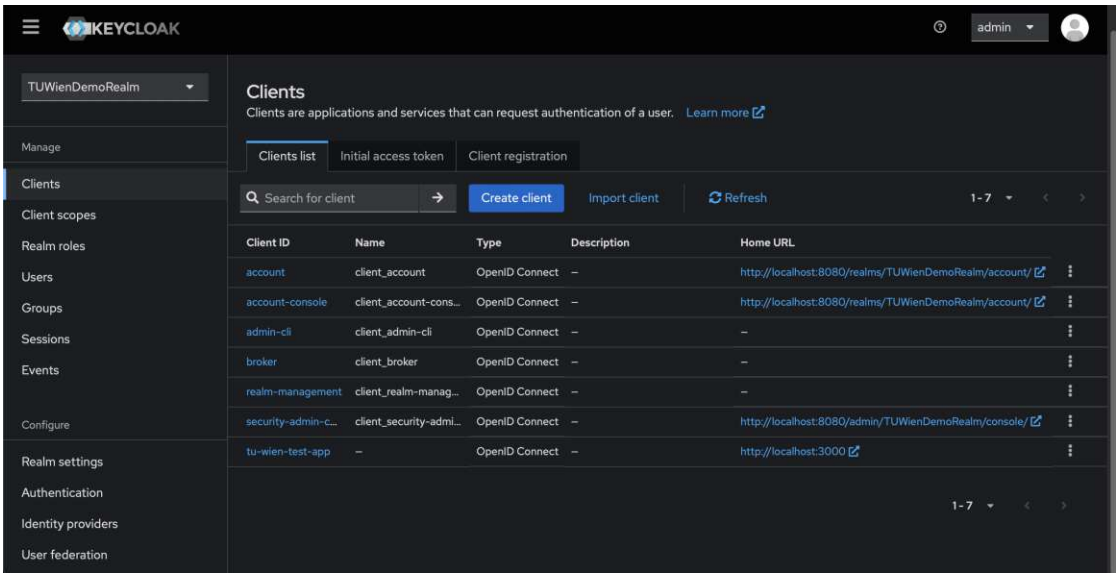


Figure 5.8: List of available clients.

Upon navigating to this account console by clicking the linked home URL in the list of available clients, the login mask as presented in Figure 5.9 is showing. Here, the created credentials for the test student user were entered.

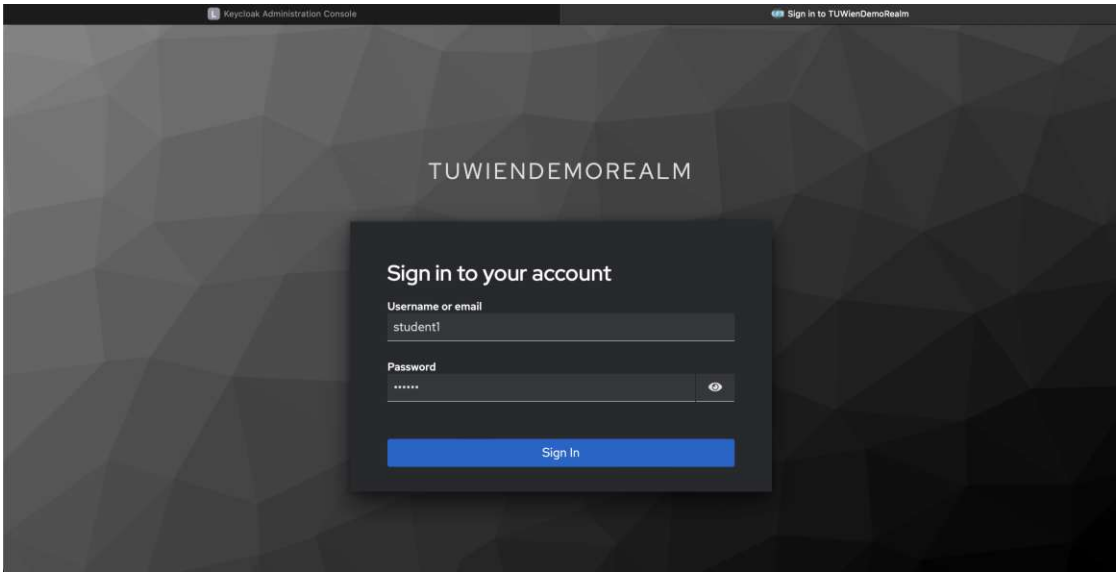
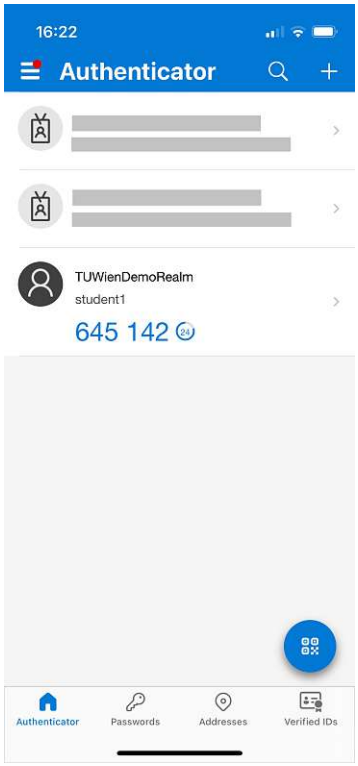


Figure 5.9: Login mask for the created demo realm.

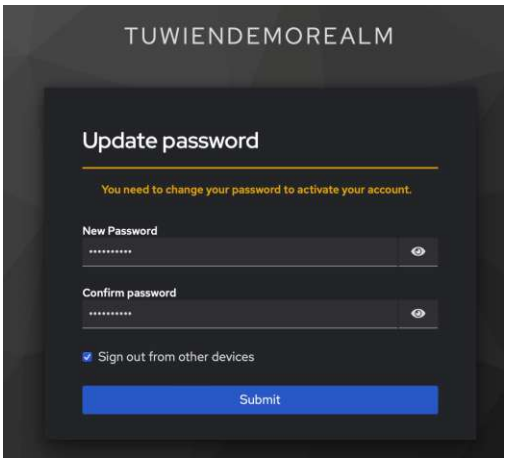
When signed in with the temporary password, a request to setup OTP via a mobile authenticator pops up immediately to activate the account. From the three options for authenticators, Microsoft Authenticator was chosen for this demonstration. The authenticator app was configured simply by scanning the QR code created by Keycloak. After entering the time-based one-time code, i.e., TOTP, the MFA setup is complete. As mentioned before, upon logging in for the first time, the temporary password needs to be updated, and the basic user data for email, first- and last-name is required. The respective screenshots for this initial login process are presented in Figure 5.10.

Eventually, the student was logged in successfully with multi-factor authentication and the account console is accessed. Figure 5.11 depicts some of the functionalities of the account console. First, a screen with a form for editing personal information is shown. Next, an overview of all accessible applications for the logged in student can be seen, which includes the sample test application "tu-wien-test-app". Furthermore, under "Account security", users can see their device/login activity and update their password. Also, they can delete existing or setup new multi-factor authentication mechanisms, i.e., setup another OTP authenticator app with the current configuration of the demonstrated Keycloak instance.

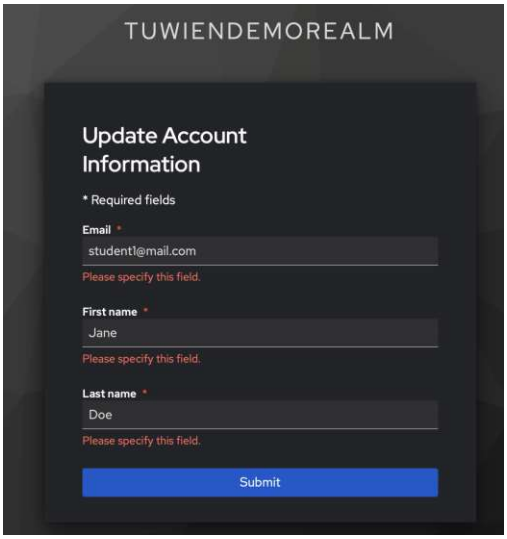
(a) Request for OTP setup.



(b) TOTP in Microsoft Authenticator.

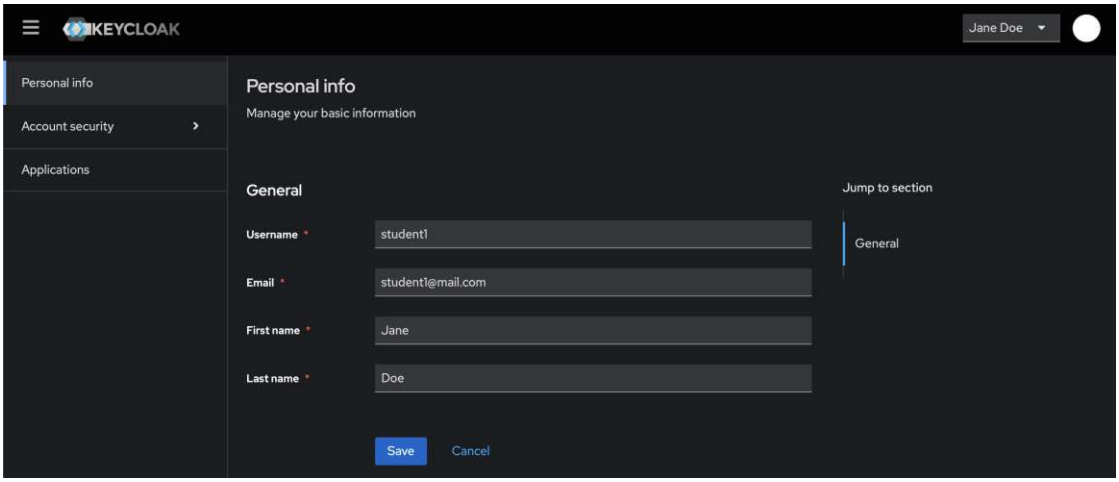


(c) Setting of a new password.

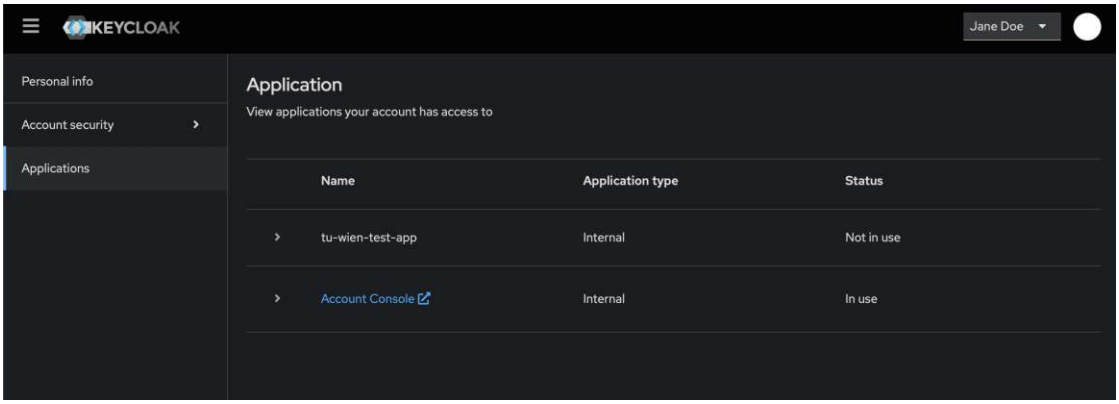


(d) Request for basic user data.

Figure 5.10: Configuration of mobile authenticator app. Also, the user is requested to set own password and basic information upon first login.



(a) Form for editing of personal information.



(b) Overview of all accessible applications.

Figure 5.11: Account-console can be accessed after successful login with MFA.

5.3 Insights and Recommendations

The presented Keycloak setup demonstrates a simplified version of a centrally hosted identity and access management (IAM) solution. It includes basic functionality of user management, multi-factor authentication using time-based one-time passwords, and the integration of web applications via OpenID Connect. The setup proved straightforward, highlighting Keycloak's ease-of-use, as can be seen in the provided screenshots. In particular, the demonstration confirmed its suitability for rapid deployment, especially when leveraging Docker-based setups.

Based on this practical evaluation, this thesis recommends that institutions, particularly academic environments like TU Wien, gradually consolidate their diverse authentication systems under a centralized IAM tool like Keycloak. An effective initial approach could be to leverage existing identity providers (IdPs), such as a SAML-based service, to manage primary authentication (username/password), with Keycloak subsequently managing MFA centrally. This would require connecting an existing IdP with Keycloak. To achieve this, the provider can be added to Keycloak by selecting and configuring supported types of providers presented in Figure 5.12. Then, Keycloak's SAML service provider metadata needs to be added to the existing SAML identity provider.[4]

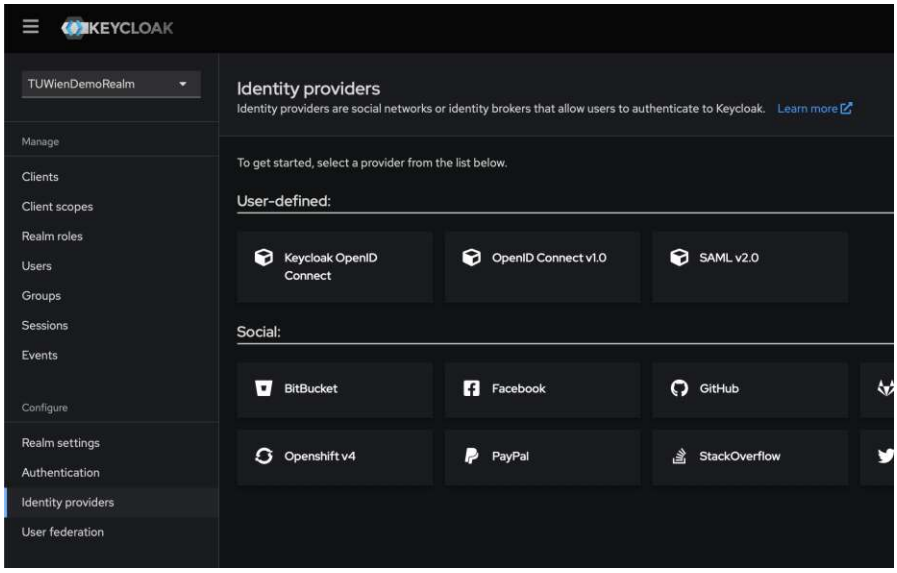


Figure 5.12: Identity providers in Keycloak.

Figure 5.13 shows a potential flow, if Keycloak is being used as an identity broker with external IdPs, as described above. This approach allows institutions to maintain their existing authentication processes initially, reducing immediate integration complexities.

[4]Integrating Identity Providers with Keycloak: `https://www.keycloak.org/docs/latest/server_admin/index.html#saml-v2-0-identity-providers`. Accessed: 2025-03-10

It also positions Keycloak as a centralized hub for managing additional authentication factors.

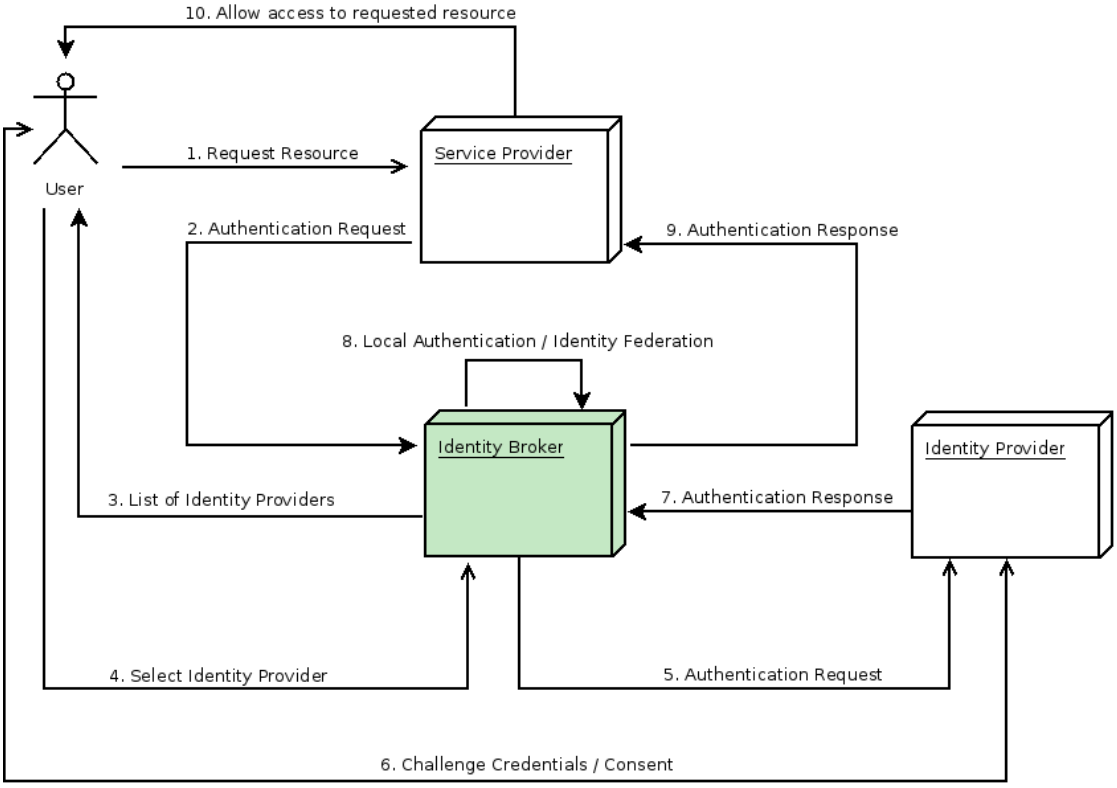


Figure 5.13: Keycloak identity broker flow. Source: `https://www.keycloak.org/docs/latest/server_admin/index.html#_identity_broker_overview`. Accessed: 2025-03-10

CHAPTER 6

Conclusion

The thesis aimed to address the need for enhancing security in academic institutions by proposing a multi-factor authentication (MFA) strategy. Through a systematic literature review and semi-structured expert interviews, a necessary understanding was developed regarding the technical, organizational, and user acceptance challenges a transition from single-factor authentication (SFA) to MFA introduces. Then, a framework analysis integrated findings from both the literature and the expert insights and resulted in a proposed strategy for implementing MFA, tailored to the unique requirements of higher education environments. Finally, a practical demonstration of Keycloak confirmed its suitability for rapid deployment. The presented Keycloak setup demonstrated a simplified version of a centrally hosted identity and access management (IAM) solution, including the setup of TOTP as second factor for authentication.

The research revealed that academic institutions face significant challenges related to technical fragmentation. Often, multiple authentication systems coexist. These range from SSO solutions based on SAML and OAuth to legacy systems such as on-premises Exchange. This fragmentation complicates the process of creating a unified MFA solution. The literature emphasizes the rising reliance on MFA to mitigate security risks, while also highlighting the need for flexible and centralized solutions, such as the open source identity and access management (IAM) solution Keycloak. The interviews further confirmed that institutions like TU Wien and other Austrian universities are actively adapting their identity management practices, though legacy systems often still yield problems. This indicates that a successful MFA strategy, from a technical perspective, must first focus on consolidating diverse authentication channels into a central platform/approach. This way security policies can be enforced in a unified process, including all necessary services. The study shows that Keycloak shows large potential in acting as this centralized IAM solution. Multiple universities are either already using it for this purpose, or are planning to do so in the near future.

Next to the technical feasibility of proper mandatory MFA rollouts, also the issue of user acceptance is critical. Especially the literature underscores that mandatory MFA can lead to frustration, stress, and even security fatigue in students. However, in this study, according to the interviewed experts of several Austrian universities, the student adoption in already existing mandatory MFA environments is overall positive. There is not much observed (and expected) resistance against the introduction of MFA. Nevertheless, the findings suggest that academic institutions, characterized by a diverse user base ranging from digital natives to non-technical users, require a user-centric approach. A phased or iterative rollout has emerged as the most effective method to enhance user adoption. This involves voluntary enrollment phases and incremental addition of services or user groups, and is always supported by comprehensive and early communication and training initiatives. It is especially important to explain to students, why MFA is necessary. This approach can mitigate the negative emotional impact associated with abrupt policy changes.

Furthermore, the research highlights the importance of offering multiple MFA methods to balance security with usability. The literature points to emerging authentication options, such as passwordless authentication, e.g., biometrics and FIDO2 keys, and adaptive authentication. These can be combined with more traditional methods like TOTP to provide a broader spectrum of choices for students and staff. Interviews with experts revealed that enabling users to select their preferred authentication method can significantly reduce friction an improve overall satisfaction. This is, again, especiall important in academic settings where the technological proficiency of users varies widely.

Particularly in the expert interviews, scalability and vendor independence emerged as additional pivotal factors in the long-term viability of an MFA solution. The open-source nature of platforms like Keycloak offers promising potential for academic institutions to maintain digital sovereignity while avoiding pitfalls of vendor lock-in. However, empirical evidence on the scalability of such solutions in large-scale academic environments remains limited. The interviews highlighted the challenges posed by limited IT staffing in contrast to very large user numbers, i.e., students numbers in the 5 to 6 figure range for large universities. Hence the necessity for iterative enhancements and the importance that the solution can adapt to evolving user demands.

In addressing the research questions, this thesis has demonstrated that implementing a unified MFA system in an academic context requires careful balancing of technical integration, user-centric design, and strategic planning. The technical challenges, such as integrating heterogeneous systems and managing legacy infrastructure, are extended by the need for scalable solutions that can accommodate a diverse user population. Overall, by centralizing identity management, adopting an iterative rollout process, enhancing user adoption through targeted communication, offering diverse authentication methods, and ensuring scalability while maintaining vendor independence, academic institutions can navigate the complex challenges of modern digital security.

CHAPTER 7

Future Work

Based on the insights of this thesis, several opportunities for future research and practical application arise. A promising area for further exploration is the evaluation of emerging authentication methods. The systematic literature review highlighted innovative techniques such as continuous authentication and adaptive methods, yet empirical data on their usability and robustness in academic settings remain limited. Future work should investigate these methods in controlled experiments and field studies, comparing their security benefits and user acceptance levels against traditional MFA approaches.

Moreover, the integration of decentralized identity management technologies, such as blockchain and self-sovereign identity (SSI), could be further explored. Although promising in theory, significant gaps remain in understanding how these approaches can be seamlessly integrated into existing academic infrastructures. Evaluating the feasibility of hybrid models that combine traditional authentication with SSI could provide valuable insights towards more resilient identity management systems.

Lastly, a cost-benefit analysis of various MFA implementation strategies in academic settings could provide valuable insights for decision-makers. Here, future work should compare the long-term financial and operational impacts of using open-source platforms like Keycloak against proprietary solutions.

In summary, the proposed directions for future research include real-world scalability assessments, in-depth evaluations of emerging authentication methods, integration of decentralized identity technologies, and comprehensive cost-benefit analyses.

APPENDIX A

Interview Guides

A.1 Preliminary Interview Guide

Background and Current Practices

1. Can you describe your role and involvement in IT security and identity management at [University Name]? **(Main Theme)**
2. Could you very briefly describe the current state of identity management and authentication mechanisms at your university? **(Main Theme)**
3. Do you use mandatory MFA at your University? If so, how long has your university been using it, and what where the initial motivations for implementing it?

Implementation Process

4. Can you walk me through the process your university followed to implement mandatory MFA? **(Main Theme)**
5. How was the rollout of MFA conducted at your institution? Did you follow a phased (gradual) or a big-bang approach?
6. At TU Wien, the existing infrastructure involves multiple authentication mechanisms across different systems (network, mail, TUaccount). How complex was/is your university's IT infrastructure? How many different identity providers, login systems/methods and applications that require logins do you use approximately?
7. What were the biggest technical and logistical challenges during the implementation process?

Keycloak

8. Does your university use Keycloak as part of your identity and access management system? If so, what role does it play in this system? If not, what other solutions are in place? **(Main Theme)**

9. What are the main advantages and limitations you've observed with using Keycloak (or alternative systems) for MFA?

10. How configurable and scalable have you found Keycloak (or alternative systems) to be, especially when it comes to integrating it with legacy systems?

User Adoption

11. How do students and staff respond to mandatory MFA? Were there significant changes in user experience? **(Main Theme)**

12. Were there any specific measures taken to minimize the invasiveness of MFA (e.g., using context-based authentication)? How strict is your MFA implementation?

13. What feedback or metrics have you gathered to evaluate user satisfaction and adoption rates, if any?

Lessons Learned

14. What key lessons did you learn from the rollout of MFA that could benefit other institutions? **(Main Theme)**

15. Do you think a phased/gradual approach is necessary for success (for a smooth transition to mandatory MFA), and why or why not?

16. In hindsight, would you change any aspect of your MFA implementation process?

17. Are there any improvements or changes planned for the current MFA system at your university?

Recommendations for TU Wien

18. Can you give any specific advice regarding TU Wien's plan to implement a unified MFA solution with Keycloak? **(Main Theme)**

A.2 Internal Interview Guide

Background and Current Practices

1. Can you describe your role and responsibilities in the area of IT security and identity management at TU Wien? **(Main Theme)**
2. How are identities currently managed? How many (and which) systems are there in total? **(Main Theme)**
3. Which authentication mechanisms are currently used for these systems?

Challenges

4. What, in your opinion, are the biggest challenges when introducing a unified MFA solution at TU Wien? **(Main Theme)**
5. Are there any technical limitations within the current infrastructure?
6. Which concerns have students or staff raised regarding mandatory MFA?
7. How do you plan to reconcile security and user-friendliness when implementing a potential MFA solution? How intrusive can the solution be?
8. How do you assess the feasibility and usefulness of context-based authentication (e.g., when users are connected to the WLAN), or limiting mandatory MFA to individual applications that require increased security? If so, which applications would those be?

Infrastructure and Integration:

9. How would you describe the complexity of the current IT infrastructure at TU Wien in the area of identity management? **(Main Theme)**
10. How many different identity providers and login systems are currently in use?
11. Which central components of the current infrastructure would need to be adapted for implementing MFA? Would you recommend a big-bang approach or a gradual, iterative approach for the integration?

Keycloak

12. Are you familiar with Keycloak? Do you consider Keycloak a suitable component for the planned MFA implementation? **(Main Theme)**
13. What specific advantages (and disadvantages) does Keycloak offer for TU Wien's use case?
14. Have any initial tests or evaluations of Keycloak already been conducted at TU Wien?

Preparation for external Interviews

15. Can you think of any questions you would like us to ask the experts at the other universities? **(Main Theme)**
16. Are there any specific challenges you would like to learn about from other universities' implementations?

A.3 Organizational Interview Guide

Background and Current Practices

1. Can you describe your role and involvement in IT security and identity management at [University Name]? **(Main Theme)**
2. Do you use mandatory MFA at your University? **(Main Theme)**
3. If so, how long has your university been using it, and what where the initial motivations for implementing it?

Implementation Process

4. What organizational strategies were employed to roll out MFA smoothly? **(Main Theme)**
5. How was the rollout of MFA conducted at your institution? Did you follow a phased (gradual) or a big-bang approach?
6. What communication strategies were most effective in gaining acceptance by students and staff?
7. How was the decision to implement mandatory MFA met? Where the students involved in this decision?

User Adoption

8. How do students and staff respond to mandatory MFA? Were there significant changes in user experience? **(Main Theme)**
9. What feedback or metrics have you gathered to evaluate user satisfaction and adoption rates, if any?
10. Were there any specific incentives that improved user compliance? How did you handle resistance?

Lessons Learned

11. What key lessons did you learn from the rollout of MFA that could benefit other institutions? **(Main Theme)**
12. Do you think a phased/gradual approach is necessary for success (for a smooth transition to mandatory MFA), and why or why not?
13. In hindsight, would you change any aspect of your MFA implementation process?
14. Are there any improvements or changes planned for the future?

Ideas for Other Universities

15. What ideas or best practices from your experience do you think could be relevant or adaptable for other universities considering a similar path? **(Main Theme)**

A.4 Technical Interview Guide

Background and Current Practices

1. Can you describe your role and involvement in IT security and identity management at [University Name]? **(Main Theme)**
2. Could you very briefly describe the current state of identity management and authentication mechanisms at your university? **(Main Theme)**
3. How complex was/is your university's IT infrastructure? How many different identity providers, authentication systems/methods and applications that require logins do you use approximately?

Implementation Process

4. Can you walk me through the technical process of implementing MFA? **(Main Theme)**
5. What tools and mechanisms does your identity management solution consist of?
6. What challenges did you face with infrastructure complexity and legacy systems?
7. If they implemented a new solution: Did you use any specific tools to manage the migration to the new solution?

Keycloak

8. Does your university use Keycloak as part of your identity and access management system? If so, what role does it play in this system? If not, what other solutions are in place? **(Main Theme)**
9. What are the main advantages and limitations you've observed with using Keycloak (or alternative systems) for MFA?
10. How configurable and scalable have you found Keycloak (or alternative systems) to be, especially when it comes to integrating it with legacy systems?

Security vs. Usability

11. How do you balance security and usability from a technical standpoint? **(Main Theme)**
12. Were there any specific measures taken to minimize the invasiveness of MFA (e.g., using context-based authentication)? How strict is your MFA implementation?
13. What specific configurations helped make MFA less invasive?

Lessons Learned

14. What key lessons did you learn from the rollout of MFA that could benefit other institutions? **(Main Theme)**
15. Are there any improvements or changes planned for the current MFA system at your university?

Ideas for Other Universities

16. What ideas or best practices from your experience do you think could be relevant or adaptable for other universities considering a similar path? **(Main Theme)**

Overview of Generative AI Tools Used

The interviews were transcribed using the integrated transcription functionality in Microsoft Teams[1].

The generative AI tool ChatGPT[2] was used for language refinement, including improvements in grammar and clarity. AI-assisted revisions focused solely on linguistic aspects, while all scientific content, interpretations, and conclusions originate from the author.

The following section was created with a generative AI tool and has been included without substantial changes:

Section: Kurzfassung

Prompt: "Please translate the following abstract to german: An increasing reliance on digital services in academic institutions and the growing [...]."

AI Tool (version), Date: ChatGPT (GPT-4o), 2025-03-16

[1] Microsoft Teams: `https://www.microsoft.com/en-us/microsoft-teams/group-chat-software`. Accessed: 2025-03-16

[2] ChatGPT: `https://chatgpt.com`. Accessed: 2025-03-16

List of Figures

List of Tables

Bibliography

[AA21] Bandar Omar ALSaleem and Abdullah I. Alshoshan. Multi-Factor Authentication to Systems Login. In *2021 National Computing Colleges Conference (NCCC)*, pages 1–4, Taif, Saudi Arabia, March 2021. IEEE.

[ABG+22] Davis Arnold, Benjamin Blackmon, Brendan Gibson, Anthony G Moncivais, Garrett B Powell, Megan Skeen, Michael Kelland Thorson, and Nathan B Wade. The Emotional Impact of Multi-Factor Authentication for University Students. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, pages 1–4, New Orleans LA USA, April 2022. ACM.

[ACS+24] Adeel Ahmad, Asier Aguado Corman, Hannah Short, Liviu Valsan, Maria Fava, Paolo Tedesco, Sebastian Lopienski, Stefan Lueders, and Vincent Brillault. The second-factor authentication system at cern. In *EPJ Web of Conferences*, volume 295, page 04025. EDP Sciences, 2024.

[Ada15] William C. Adams. *Conducting Semi-Structured Interviews*, chapter 19, pages 492–505. John Wiley & Sons, Ltd, 2015.

[AK22] Jason Anderson and Kate Keahey. Migrating towards Single Sign-On and Federated Identity. In *Practice and Experience in Advanced Research Computing*, pages 1–8, Boston MA USA, July 2022. ACM.

[AP20] Jacob Abbott and Sameer Patil. How Mandatory Second Factor Affects the Authentication User Experience. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, Honolulu HI USA, April 2020. ACM.

[BKCK24] Christian Baun, Martin Kappes, Henry-Norbert Cocos, and Malte Martin Koch. Eine Plattform zur Erstellung und Verwendung komplexer virtualisierter IT-Strukturen in Lehre und Forschung mit Open Source Software: Erfahrungen bei der Entwicklung und Nutzung einer neuen Plattform zur Digitalisierung der Hochschullehre. *Informatik Spektrum*, 47(1-2):38–45, April 2024.

[CAS+17] Marcus Christie, Anuj Bhandar, Supun Nakandala, Suresh Marru, Eroma Abeysinghe, Sudhakar Pamidighantam, and Marlon Pierce. Using Keycloak

for Gateway Authentication and Authorization. *Presented at Gateways 2017, University of Michigan*, 2017.

[CFS+23] Argyris Constantinides, José Faria, Taoufik Sousak, Pedro Martins, David Portugal, Marios Belk, Andreas Pitsillides, and Christos Fidas. TRUSTID: Intelligent and Continuous Online Student Identity Management in Higher Education. In *Adjunct Proceedings of the 31st ACM Conference on User Modeling, Adaptation and Personalization*, pages 110–114, Limassol Cyprus, June 2023. ACM.

[DC20] Divyabharathi D. N. and Nagaraj G. Cholli. A Review on Identity and Access Management Server (KeyCloak):. *International Journal of Security and Privacy in Pervasive Computing*, 12(3):46–53, July 2020.

[EHH19] Mohammad El Hajj Hussein. Reproducible examples for integration with keycloak. Technical report, CERN, Geneva, 2019.

[FBPP21] Christos Fidas, Marios Belk, David Portugal, and Andreas Pitsillides. Privacy-preserving Biometric-driven Data for Student Identity Management: Challenges and Approaches. In *Adjunct Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization*, UMAP '21, pages 368–370, New York, NY, USA, June 2021. Association for Computing Machinery.

[Gol21] Laurie J Goldsmith. Using Framework Analysis in Applied Qualitative Research. *Qualitative report*, 26(6), 2021.

[HPTK23] Die Hu, Danaitun Pongpatcharatrontep, Somhatai Timsard, and Achara Khamaksorn. Blockchain Applications in Higher Education: A Systematic Literature Review. In *2023 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON)*, pages 188–193, Phuket, Thailand, March 2023. IEEE.

[Kit04] Barbara Kitchenham. Procedures for Performing Systematic Reviews. *Keele, UK, Keele Univ.*, 33, 08 2004.

[KPJK16] Hanna Kallio, Anna-Maija Pietilä, Martin Johnson, and Mari Kangasniemi. Systematic Methodological Review: Developing a Framework for a Qualitative Semi-Structured Interview Guide. *Journal of advanced nursing*, 72(12):2954–2965, 2016.

[KS22] Yoshiaki Kasahara and Takao Shimayoshi. Our Design and Implementation of Multi-Factor Authentication Deployment for Microsoft 365 in Kyushu University. In *Proceedings of the 2022 ACM SIGUCCS Annual Conference*, pages 56–61, Virtual Event USA, March 2022. ACM.

[Lin22] Steve Linthicum. The Need for Multifactor Authentication for Higher Ed. https://ransomware.org/blog/the-need-for-multifactor-authentication-for-higher-ed/, 2022. Accessed: 2024-05-26.

[NMA23] Takahiro Nemoto, Kazuhiro Mishima, and Shigeyoshi Aoyama. Implementation and Initial Operation of IDaaS as Integrated Authentication Infrastructure in TUAT. In *Proceedings of the 2023 ACM SIGUCCS Annual Conference*, pages 48–52, Chicago IL USA, March 2023. ACM.

[Now23] Karol Nowak. What is Keycloak: Unlocking the Power of a Comprehensive Identity and Access Management Solution. https://inteca.com/blog/2023/04/26/what-is-keycloak-unlocking-the-power-of-a-comprehensive-identity-and-access-management-solution/, 2023. Accessed: 2024-10-18.

[PJJ21] Davy Preuveneers, Sander Joos, and Wouter Joosen. AuthGuide: Analyzing Security, Privacy and Usability Trade-Offs in Multi-factor Authentication. In Simone Fischer-Hübner, Costas Lambrinoudakis, Gabriele Kotsis, A Min Tjoa, and Ismail Khalil, editors, *Trust, Privacy and Security in Digital Business*, volume 12927, pages 155–170. Springer International Publishing, Cham, 2021.

[RJ23] Midhuna Jyothi R and N. Jeyanthi. A Review of Modern Authentication Methods in Digital Systems. In *2023 Annual International Conference on Emerging Research Areas: International Conference on Intelligent Systems (AICERA/ICIS)*, pages 1–6, Kanjirapally, India, November 2023. IEEE.

[ST08] Aashish Srivastava and Stanley Thomson. Framework Analysis: A Qualitative Methodology for Applied Policy Research. *JOAAG*, 4, 11 2008.

[STK+24] Rostyslav Shchokin, Valentyn Teslenko, Viktoriia Krykun, Anatolii Balashov, Inna Semenets-Orlova, and Alla Klochko. Digitalization Trends in Higher Education. In Rostyslav Shchokin, Anna Iatsyshyn, Valeriia Kovach, and Artur Zaporozhets, editors, *Digital Technologies in Education*, volume 529, pages 55–66. Springer Nature Switzerland, Cham, 2024.

[TS21] Stian Thorgersen and Pedro Igor Silva. *Keycloak-identity and access management for modern applications: harness the power of Keycloak, OpenID Connect, and OAuth 2.0 protocols to secure applications*. Packt Publishing Ltd, 2021.

[WW02] Jane Webster and Richard T. Watson. Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, 26(2):xiii–xxiii, 2002.

[YRN+21] Hakan Yildiz, Christopher Ritter, Lan Thao Nguyen, Berit Frech, Maria Mora Martinez, and Axel Kupper. Connecting Self-Sovereign Identity with Federated and User-centric Identities via SAML Integration. In *2021 IEEE*

Symposium on Computers and Communications (ISCC), pages 1–7, Athens, Greece, September 2021. IEEE.

[Zim18] Eli Zimmerman. Education Department Warns Universities to Improve Identity Management. https://edtechmagazine.com/higher/article/2018/10/education-department-warns-universities-improve-identity-management, 2018. Accessed: 2024-05-26.