Hochschulforum Digitalisierung

DISKUSSIONSPAPIER NR. 24 / JULI 2023

Digitale Prüfungen mit Bring Your Own Device (BYOD)

In diesem Diskussionspapier wird mit dem FLEX-Framework eine Lösung für die Nutzung von BYOD-Ansätzen einhergehenden Herausforderungen erörtert. Zuverlässigkeit und Sicherheit vor Prüfungsbetrug sind in diesem Zusammenhang Themen von besonderem Interesse. Gleichzeitig bietet das Framework Potentiale für den Einsatz von praxisnahen und kompetenzorientierten Prüfungsaufgaben.

Autor

Bastian Küppers, RWTH Aachen

1. Warum digitale Prüfungen mit Bring Your Own Device?

Elektronische bzw. Digitale Prüfungen (am Campus) sind kein neues Thema im Hochschulkontext. Im Rahmen der Corona-Pandemie hat die Thematik aber an Bedeutung gewonnen. Allerdings gibt es noch keinen „gemeinsamen Weg" für die Durchführung elektronischer Prüfungen. Gleichzeitig wird durch die Beibehaltung von bzw. Rückkehr zu Papierklausuren deutlich, dass es noch viele Vorbehalte gegenüber digitalen Prüfungen gibt. Zu diesen Vorbehalten gehören die (vermeintlich mangelnde) Fairness digitaler Prüfungen oder die (fehlende) Zuverlässigkeit digitaler Prüfungssystem. Digitale Prüfungen bringen jedoch erhebliche Vorteile mit sich, sodass sie in jedem Fall ein integraler Bestandteil der Prüfungskultur an Hochschulen sein sollten.

Oft gründen sich die Vorbehalte gegenüber elektronischen Prüfungen auf Vorurteile, deren Abbau ein wichtiger Schritt auf dem Weg zu einer größeren Verbreitung elektronischer Prüfungen ist. Häufig sind aber auch finanzielle Gründe ein Hindernis, da die Anschaffung und Wartung elektronischer Infrastruktur ein teures Unterfangen ist.

Der größte Nachteil ergibt sich jedoch für die Studierenden, da sie in einer ungewohnten Arbeitsumgebung ihre Prüfungsleistung ablegen müssen. Da allerdings die meisten Studierenden bereits über eigene Hardware verfügen, die leistungsstark genug ist, um elektronische Prüfungen (engl. *electronic assessment*, EA) darauf durchzuführen zu können [1, 2, 3], ist ein Bring-Your-Own-Device-Ansatz eine mögliche Lösung für dieses Problem. In einem solchen Szenario können die Studierenden die Prüfungen in einer gewohnten Arbeitsumgebung ablegen. Dies stellt voraussichtlich den größten Vorteil aus Sicht der Studierenden dar, da sie so in einer Prüfungssituation nicht auch noch mit einer ungewohnten Arbeitsumgebung konfrontiert sind.[1]

2. Varianten für den Einsatz von BYOD

Betrachtet man bereits implementierte Lösungen für elektronische Prüfungen mit einem BYOD-Ansatz, so stellt man fest, dass sich diese Lösungen hauptsächlich in zwei Punkten unterscheiden:

1. Welche Software wird auf den Endgeräten der Studierenden verwendet?
2. Sind die Endgeräte der Studierenden mit einem Netzwerk verbunden und wenn ja, wie sieht diese Verbindung aus?

Ganz grundsätzlich können die Endgeräte der Studierenden entweder als Workstation oder als Client für eine Serverinfrastruktur genutzt werden [4]. Die Geräte können dabei entweder per Kabel mit einem Netzwerk, per WLAN oder gar nicht verbunden werden.

Wenn die Geräte der Studierenden als **Workstations** verwendet werden, wird die während der elektronischen Prüfung verwendete Software auf den Geräten der Studierenden installiert und ausgeführt. Hierfür gibt es verschiedene Ansätze, die sich im Grad der Freiheit der Studierenden und in den Möglichkeiten, Vorkehrungen gegen Betrug zu treffen, unterscheiden [5]. Um es den Prüfenden leichter zu machen, kann von den Studierenden verlangt werden, dass sie eine bestimmte Software verwenden, die seitens der Hochschule bereitgestellt wird. Die Verpflichtung der Studierenden, während

[1] Eine detaillierte Diskussion über die Vorurteile und Vorteile digitaler Prüfungen wird in [6] geführt.

einer elektronischen Prüfung eine bestimmte Software zu verwenden, z. B. NetBeans für einen Programmierkurs, bietet jedoch keine Sicherheit. Daher wird neben den erforderlichen Werkzeugen oft eine so genannte LockDown-Software für die Prüfung verlangt, z. B. Safe Exam Browser. Dieser Ansatz wirft jedoch potenzielle Probleme hinsichtlich der Softwarekompatibilität auf, da alle Studierenden in der Lage sein müssen, die LockDown-Software auf ihren Geräten auszuführen. Dies kann zu einem Problem werden, wenn das Betriebssystem einzelner Studierender nicht von der Software unterstützt wird.

Die Geräte der Studierenden als **Clients** zu verwenden, ist eine weitere Möglichkeit zur Umsetzung des BYOD-Ansatzes für elektronische Prüfungen. Das bedeutet, dass nicht die Hardware der Geräte selbst zum Arbeiten verwendet wird, sondern das Gerät als Verbindung zu einer zentralen IT-Infrastruktur fungiert, wie z. B. einem Remote-Desktop-Server. In solchen Szenarien haben die Prüfenden die volle Kontrolle über die Arbeitsumgebung selbst und können eine vorkonfigurierte Umgebung bereitstellen. Außerdem stehen den Prüfenden die Ergebnisse der Studierenden auf dem Remote-Server zur Verfügung und müssen nicht über USB-Sticks oder Ähnliches eingesammelt werden. Dieses Szenario ist jedoch vergleichsweise anfällig für Prüfungsbetrug, da die Studierenden außerhalb der Client-Software arbeiten können, sofern keine weiteren Vorkehrungen getroffen werden. Diese Vorkehrungen führen jedoch zu den gleichen Problemen, wie sie bereits für die Nutzung der Geräte der Studierenden als Workstations diskutiert wurden.

Neben den oben erwähnten gibt es technisch noch weitere Möglichkeiten, um eine Verbindung mit den Geräten der Studierenden herzustellen, z. B. über ein Mobilfunknetz. Diese Art der Verbindung ist jedoch für elektronische Prüfungen nicht geeignet, da sie nicht unter der Kontrolle der Prüfenden steht. Je nach gewähltem BYOD-Ansatz ist es nicht notwendig, dass die Geräte der Studierenden überhaupt mit einem Netzwerk verbunden sind, z. B. wenn die Studierenden die Software, mit der sie arbeiten wollen, selbst auswählen können oder wenn ein komplettes Betriebssystem auf einem USB-Stick zur Verfügung gestellt wird, der auch zur Erfassung der Ergebnisse verwendet wird. Netzwerkzugriff der Geräte kann jedoch erforderlich sein, wenn die Ergebnisse der Studierenden über ein LMS bereitgestellt werden sollen oder wenn Online-Materialien zugänglich sein müssen. Wenn die Geräte an ein lokales Netzwerk, entweder per Kabel oder per Wi-Fi, angeschlossen sind, kann dieses Netzwerk einen durch eine Firewall kontrollierten Internetzugang erlauben. Ob eine Verbindung zum Internet notwendig ist, hängt vom gewählten Ansatz für die elektronischen Prüfungen ab. Wenn die Geräte der Studierenden als Clients verwendet werden, ist eine Verbindung zum Internet nicht zwingend erforderlich, eine Verbindung zum Netzwerk der Hochschule ist prinzipiell ausreichend. Die Verbindung mit dem Netzwerk der Hochschule ohne Internetzugang hindert die Studierenden jedoch nicht daran, miteinander zu kommunizieren. Um dies zu verhindern, muss das Netzwerk entsprechend konfiguriert werden.

Außerdem müssen andere Kommunikationsmethoden, wie Bluetooth oder LTE, unterbunden werden. Letzteres kann durch bauliche Maßnahmen verhindert werden, zum Beispiel durch den Bau von Prüfungsräumen, die einem Faraday'schen Käfig ähneln. Lokal aufgebaute Bluetooth-Verbindungen können von den Prüfenden beispielsweise erkannt werden, indem sie selbst nach solchen Verbindungen suchen. Mehr Details zu den einzelnen Varianten elektronische Prüfungen mit einem BYOD-Ansatz umzusetzen, werden in [7, 8] beschrieben.

3. Anforderungen für den Einsatz von BYOD in Prüfungen

Auf Basis dieser Überlegungen wurde an der RWTH Aachen ein Framework für elektronische Prüfungen mit einem BYOD-Ansatz entwickelt. Framework bedeutet in diesem Kontext: Ein Paket, bestehend aus der Software zur Durchführung elektronischer Prüfungen sowie den formalen Bedingungen, die erfüllt sein müssen, um Prüfungen an einer Hochschule rechtssicher durchführen zu können. Insbesondere die Aspekte Sicherheit und Gleichbehandlung mussten dabei berücksichtigt werden. Zusätzlich wurden die Anforderungen aller beteiligten Statusgruppen-Parteien (Lehrende, Studierende, technisches Personal) erhoben, die sich aus Gesetzen und Regularien ergeben und für die erfolgreiche Durchführung elektronischer Prüfungen berücksichtigt werden müssen.

Im Folgenden werden einige Termini häufiger vorkommen, daher werden diese hier zum besseren Verständnis kurz definiert:

EA-Framework	Das Gesamtpaket aus Prüfungssoftware und formalen Anforderungen.
EA-Software	Die komplette Prüfungssoftware, bestehend aus Client und Server.
EA-App	Der Client, der auf den Endgeräten der Studierenden ausgeführt wird.
EA-Server	Die vollständige Serverinfrastruktur, zu der sich die EA-App verbindet.

Für die praktische Umsetzung von elektronischen Prüfungen ist es wichtig, dass sowohl Prüfende als auch Studierende diese als Teil des Hochschulprüfungssystems akzeptieren [9]. Daher ist es erforderlich, die Bedenken von Prüfenden und Studierenden zu sammeln und zu analysieren. So kann eine EA-Software entwickelt werden, die an der Hochschule allgemein akzeptiert und erfolgreich eingesetzt wird. Dieser Prozess ist dem *Requirements Engineering* in der Softwareentwicklung sehr ähnlich.

Laut Lukarov gibt es drei Hauptgruppen von Interessenvertretern und Entscheidungsträgern: Studierende, Lehrkräfte und Verwaltungsorgane [10]. Im Rahmen des *Requirements Engineering*[2] wurden Studierende und Lehrende unterschiedlicher Hochschulen befragt. Anforderungen der Verwaltungsorgane wurden am Beispiel der RWTH Aachen auf Basis veröffentlichter Strategie- und Policypapers erhoben.[3]

[2] Das *Requirements Engineering* wurde im Rahmen des MATSE-Ausbildungsprogramms an der RWTH Aachen durchgeführt. MATSE ist die Abkürzung für Mathematisch Technischer Software Entwickler. Dieser Ausbildungsgang umfasst eine Berufsausbildung in einer Forschungseinrichtung oder einem Unternehmen und den Bachelor-Studiengang Angewandte Mathematik und Informatik. (Angewandte Mathematik und Informatik, früher *Science Programming*) an der FH Aachen [11].

[3] Eine tiefergehende Auseinandersetzung mit der Befragung von Studierenden und Prüfenden findet sich in [12].

3.1. Anforderungen von Studierenden

Die Ergebnisse der Studierendenumfrage zeigen ein recht klares Bild: Die Studierenden hätten gerne elektronische Prüfungen in ihren Studiengängen. Allerdings wünschen sich die Teilnehmenden diese nicht unbedingt als Ersatz für Papierklausuren, sondern eher als Ergänzung. Diese Wahrnehmung von elektronische Prüfungen scheint von den Vorteilen, die sie bieten, bestimmt zu sein. Genannt werden Themen wie schnelle Korrektur, realistischere Aufgaben, vielfältige Prüfungsaufgaben und Lesbarkeit. Die Studierenden machen sich jedoch auch Gedanken über Nachteile wie Sicherheit, Nutzbarkeit und Fairness. Gerade bei einem BYOD-Ansatz befürchten die Studierenden, dass technische Schwierigkeiten zu einem Handicap für sie führen könnten oder dass sie selbst ein leistungsfähiges Gerät besitzen müssen. Dennoch gibt es eine positive Tendenz bezüglich eines BYOD-Ansatzes, da die Studierenden den Vorteil eines vertrauten Geräts in der Prüfung sehen. Darüber hinaus sind Themen wie Sicherheit und Prüfungsbetrug für die Studierenden von Bedeutung. Die Studierenden sind recht geteilter Meinung über das Risiko von Prüfungsbetrug bei Papierprüfungen. Jedoch gibt es unter ihnen eine Tendenz zu glauben, dass Betrügen in elektronischen Prüfungen einfacher sei.

Die Studierenden bewerten also viele Eigenschaften von elektronischen Prüfungen und BYOD als durchaus positiv. Allerdings äußern die Teilnehmenden der Umfrage auch eine Reihe von Bedenken, wie z. B. Systemabstürze und den damit verbundenen Verlust von Daten oder allgemeine Bedenken

Folgende Aspekt sind für das Framework zu berücksichtigen:

1. Es müssen Strategien verfügbar sein, um . . .
    a. . . . Studierende, die kein geeignetes Gerät besitzen, zu unterstützen
    b. . . . technische Probleme während der Prüfung zu lösen.
2. Die EA-Software muss . . .
    a. . . . eine gute Benutzerfreundlichkeit bieten.
    b. . . . frei verfügbar sein, damit sich die Studierenden vor der Prüfung damit vertraut machen können.
    c. . . . von den Studierenden überprüfbar sein.
3. Es müssen Maßnahmen ergriffen werden, um . . . zu verhindern.
    a. . . . unfaire Vorteile für bestimmte Studierende
    b. . . . Betrug während der elektronischen Prüfungen
    c. . . . Manipulation der eingereichten Antworten
    d. . . . Datenverlust während der Prüfung, z. B. durch einen Systemabsturz
4. Der gesamte Prozess für elektronische Prüfungen muss für die Studierenden transparent sein.

hinsichtlich Sicherheit und Betrug. Dies deckt sich mit anderen Studien von Kocdar et. al. [13] und Hillier et. al [14]. Basierend auf all diesen Aspekten, die von Studierenden als positiv oder negativ wahrgenommen werden, ist es wichtig, beide Seiten im Konzept eines Frameworks anzusprechen, um sicherzustellen, dass Studierende elektronische Prüfungen mit einem BYOD-Ansatz akzeptieren. Einige Aspekte können jedoch nicht durch ein Rahmenkonzept beeinflusst werden, z. B. die Wahrnehmung der Art des Schreibens (Stift vs. Tastatur) in dieser Prüfungsform.

3.2. Anforderungen von Prüfenden

Der verfügbaren Literatur zufolge ist die Haltung der Prüfenden gegenüber elektronischen Prüfungen eher zurückhaltend [15]. Ein Hauptgrund dafür sind die Betrugsmöglichkeiten, die bei elektronischen Prüfungen mutmaßlich zunehmen könnten [16]. Die Prüfenden sind sich im Allgemeinen einig, dass elektronische Prüfungen eine gute Ergänzung zur Papierklausuren sind, während ihre Einschätzung zu den Täuschungsmöglichkeiten keine klare Tendenz erkennen lässt. Allerdings scheint es einen Konsens zu geben, dass es in elektronischen Prüfungen leichter ist zu schummeln als in einer Papierklausur. Dies deckt sich mit Erkenntnissen aus der Literatur [17, 18].

Aus den gesammelten Daten lassen sich einige Aspekte ableiten, die von den Prüfenden als kritisch angesehen werden. Die Prüfenden sehen aber auch positive Aspekte von elektronischen Klausuren, wie z. B. ein besseres Prüfungsmanagement, einschließlich Studierendenverwaltung und Statistiken, und innovative Aufgaben, möglicherweise einschließlich multimedialer Inhalte. Auf der anderen Seite sind die Prüfenden bei bestimmten Aufgabentypen unsicher, ob diese für eine elektronische Prüfung geeignet sind. Insgesamt halten sich die positiven und negativen Aspekte von elektronischen Prüfungen die Waage, aber wenn es um elektronische Prüfungen mit einem BYOD-Ansatz geht, lehnen die Prüfenden diese Idee eindeutig ab. Von den Prüfenden wurden nahezu keine positiven Aspekte

Folgende Aspekt sind für das Framework zu berücksichtigen:

1. Die EA-Software muss . . .

    a. . . . eine Möglichkeit bieten, die Prüfungsverwaltung komfortabel durchzuführen (Studierende anmelden, Aufgaben erstellen, korrigieren, archivieren, ...).

    b. . . . eine Softwareschnittstelle zur Implementierung und Anpassung von Aufgabentypen an die Bedürfnisse der Prüfenden bieten.

2. Es müssen Maßnahmen ergriffen werden, um zu verhindern, dass . . .

    a. . . . unfaire Vorteile für bestimmte Studierende entstehen.

    b. . . . Prüfungsbetrug begangen wird.

    c. . . . Lösungen der Studierenden im Nachgang manipuliert werden.

    d. . . . es während der Prüfungen zu Datenverlust kommt, z. B. durch einen Systemabsturz.

3. Der gesamte Prozess für elektronische Prüfungen muss für die Prüfenden transparent sein, um Zweifel ausräumen.

genannt und die meisten negativen Aspekte betreffen die Möglichkeit des Prüfungsbetrugs. Es ist daher sehr wichtig, diese Aspekte im Konzept eines Frameworks zu berücksichtigen, um die Prüfenden davon zu überzeugen, dass elektronische Prüfungen mit einem BYOD-Ansatz erfolgreich umgesetzt werden können, ohne Prüfungsbetrug Tür und Tor zu öffnen.

3.3. Hochschulverwaltung

An der RWTH Aachen hat die Hochschulverwaltung im Rahmen der Digitalisierungsstrategie der Lehre öffentlich bekannt gegeben, welche Anforderungen sie bei elektronischen Prüfungen als wichtig erachten [19, 20]. Darüber hinaus wurden die datenschutzrechtlichen Anforderungen an der RWTH Aachen in der E-Learning-Verordnung [21] veröffentlicht. In den Dokumenten werden damit Rahmenbedingungen für elektronische Prüfungen an der RWTH Aachen formuliert. Es wird festgehalten, dass „ein Konzept zur Bereitstellung der notwendigen Infrastruktur für die umzusetzenden Blended Learning Aktivitäten abgestimmt und eine dauerhafte Finanzierung gewährleistet" werden muss. „Die Infrastruktur umfasst z. B. die bestehende und zukünftige Hörsaalausstattung, flachendeckendes WLAN, die Möglichkeiten zur Durchführung elektronischer Prüfungen inklusive der Ausstattung mit der notwendigen Hardware" [20, S. 7]. Darüber hinaus legt die E-Learning-Verordnung explizit fest, welche Datensicherheitsmaßnahmen für ein E-Learning-System getroffen werden müssen.

Es müssen Maßnahmen getroffen werden, um sicherzustellen, dass . . .

1. … „die Zweckbindung erhobener Daten gewährt wird" [21, S. 6]
2. … „ausschließlich die Berechtigten auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können" [21, S. 6]
3. … „nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder gelöscht und an welche Stellen sie weitergegeben worden sind" [21, S. 6]
4. … „personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind" [21, S. 6]

3.4. Sicherheitsanforderungen

Sicherheitsbedrohungen gibt es bei jeder Prüfungsform, und sie werden von den Studierenden ausgenutzt [22]. Bei der Einführung von elektronischen Prüfungen eröffnet die Verwendung von Computern neue Betrugsrisiken – theoretisch.

Diese potenzielle Bedrohung scheint sich bei einem BYOD-Ansatz noch zu verschärfen, da die Geräte der Studierenden generell nicht als *trusted devices* betrachtet werden können. Abgesehen von dieser Argumentation scheint es jedoch vernünftig, davon auszugehen, dass Betrug etwas ist, das ein gutes Kosten-Nutzen-Verhältnis haben muss. Danach würden sich die Studierenden dafür entscheiden, auf

eine Weise zu betrügen, die ihnen den bestmöglichen Vorteil während der Prüfung verschafft, vorausgesetzt, die gewählte Art des Betrugs führt nicht zu einem zu großen Aufwand und - was vielleicht noch wichtiger ist - zu einem höheren Risiko, erwischt zu werden. In gewisser Hinsicht ist es immer noch einfacher, ein Smartphone auf der Toilette zu benutzen, als eine digitale Prüfungssoftware nachzubauen oder zu hacken. Die Maßnahmen gegen Betrug sollten also sehr ähnliche Charakteristik aufweisen wie der Betrug selbst: Sie sollte ein gutes Kosten-Nutzen-Verhältnis haben. Da absolute Sicherheit nicht möglich ist, wie der Sicherheitsexperte Bruce Schneier betont hat, ist absolute Sicherheit auch nicht das Ziel, das man anstreben sollte. Andererseits scheint es für Prüfende und technisches Personal inakzeptabel, keine Sicherheitsmaßnahmen zu ergreifen. Es muss also das richtige Maß an Maßnahmen definiert werden, das einerseits nicht zu viel Aufwand für Entwicklung und Betrieb erfordert, andererseits aber ausreichende Sicherheit bietet. Dies wiederum basiert auf der Annahme, dass elektronische Prüfungen ein ähnliches Maß an Sicherheit bieten müssen wie papierbasierte Prüfungen. Um jedoch sinnvolle Sicherheitsanforderungen ableiten zu können, muss zunächst ein *threat model* entwickelt werden, das als Argumentationsgrundlage dienen kann. Auf der Grundlage der Arbeiten von Sindre und Vegendla [23] wurde ein *threat model* entwickelt, das aus den folgenden Bedrohungen besteht:

- Vortäuschung einer anderen Identität
- Unerlaubte Hilfestellung / Kollaboration
- Plagiarismus
- Verwendung nicht erlaubter Hilfsmittel
- Überschreitung des Zeitrahmens
- Belügen der Aufsichten
- Unerlaubtes entwenden der Klausurfragen nach der Klausur
- Manipulation eingereichter Lösungen

Aus diesen Bedrohungen lassen sich Sicherheitsanforderungen ableiten, die eine Softwarelösung erfüllen muss, um nicht gegen die identifizierten Bedrohungen vulnerabel zu sein. Für jede der identifizierten Bedrohungen konnten Gegenmaßnahmen ermittelt werden. An dieser Stelle ist es wichtig zu erwähnen, dass diese Gegenmaßnahmen nicht ausschließlich technischer Natur sind, sondern in einigen Fällen formale Anforderungen darstellen, die in die Prüfungsprozesse der Hochschule implementiert werden müssen.

Im Einzelnen wurden die folgenden Anforderungen abgeleitet:

1 Die EA-Software muss . . .

a. . . . die Ergebnisse der Studierende automatisch persönlich kennzeichnen.

b. . . . muss in der Lage sein, Studierende zu authentifizieren.

c. . . . die Ergebnisse der Studierende mit einem digitalen Zertifikat signieren.

d. . . . die Prüfungsaufgaben nur in einem begrenzten Zeitrahmen zur Verfügung stellen.

e. . . . die Lösungen der Studierende am Ende der Prüfung automatisiert einsammeln.

f. . . . verhindern, dass die Studierenden die Prüfungsfragen kopieren.

g. . . . Studierenden Quittungen aushändigen, um zu beweisen, dass diese ihre Lösungen abgegeben haben.

2. Es müssen Maßnahmen ergriffen werden, um zu verhindern, dass . . .

a. . . . Plagiate als Lösungen eingereicht werden.

b. ... die Prüfungssoftware manipuliert wird.

c. . . . verbotene Handlungen während der Prüfung begangen werden, beispielsweise die Nutzung unerlaubter Webseiten.

3.5. Technische Anforderungen

Einige der gesammelten Anforderungen haben einen erheblichen Einfluss auf die Softwarearchitektur, sowie auf die Wahl der Programmiersprache, für die EA-Software.

Um die Unterschiede zwischen den Geräten der Studierenden auszugleichen, kann ein Konzept namens *computational offloading*, das aus dem Bereich des *mobile computing* stammt, verwendet werden [24, 25]. Bei diesem Ansatz wird ein per Netzwerk angebundenes System verwendet, das genügend Verarbeitungskapazitäten bietet, um rechenintensive Aufgaben auszuführen. Obwohl dieses Prinzip für Smartphones und Tablets entwickelt wurde, kann es auch auf Notebooks und andere mobile Geräte angewendet werden. Bei elektronischen Prüfungen werden die Unterschiede zwischen den Geräten der Studierenden durch die Auslagerung von Berechnungen wirksam verringert, da alle Studierenden für rechenintensive Aufgaben auf dieselben Server angewiesen sind. Die Architektur der EA-Software muss so konzipiert sein, dass sie die Auslagerung von Berechnungen ermöglicht.

Ebenso muss die Architektur in der Lage sein, eine Integritätsprüfung des EA-Clients auf den Geräten der Studierenden durchzuführen.

Es gibt mehrere Möglichkeiten, verschiedene Betriebssysteme mit einer Software zu unterstützen. Eine Möglichkeit ist die Erstellung unterschiedlicher Quellcodes für die verschiedenen Betriebssysteme. Das hat den Vorteil, dass man die verschiedenen Programme auf das jeweilige Zielbetriebssystem abstimmen kann. Die verschiedenen Quellcodes könnten sogar in verschiedenen Programmiersprachen geschrieben werden. Dieser Ansatz ermöglicht also maximale Flexibilität im Entwicklungsprozess. Allerdings ist dieser Ansatz mit einem hohen Zusatzaufwand verbunden, da jede neue Funktion für verschiedene Betriebssysteme separat implementiert werden muss. Dies ist möglicherweise der Grund, warum die bestehende LockDown-Software nicht für jedes Betriebssystem verfügbar ist. Da dieser Ansatz zu viel Aufwand bedeutet, ist er nicht wirtschaftlich und es wird eine andere Lösung benötigt, zum Beispiel ein Programm-Framework, das für alle vorgesehenen Betriebssysteme verfügbar ist.

4. Implementierung von FLEX

Auf der Grundlage der im Rahmen der Anforderungsanalyse gesammelten Anforderungen wurde **FLEX** (**F**ramework **F**or **FLE**xible **E**lectronic **EX**aminations) entwickelt. Die grundlegende Architektur des EA-Frameworks ist in Abb. 1 dargestellt. Die vier Komponenten dieser Architektur werden in den nächsten Abschnitten erläutert[4].

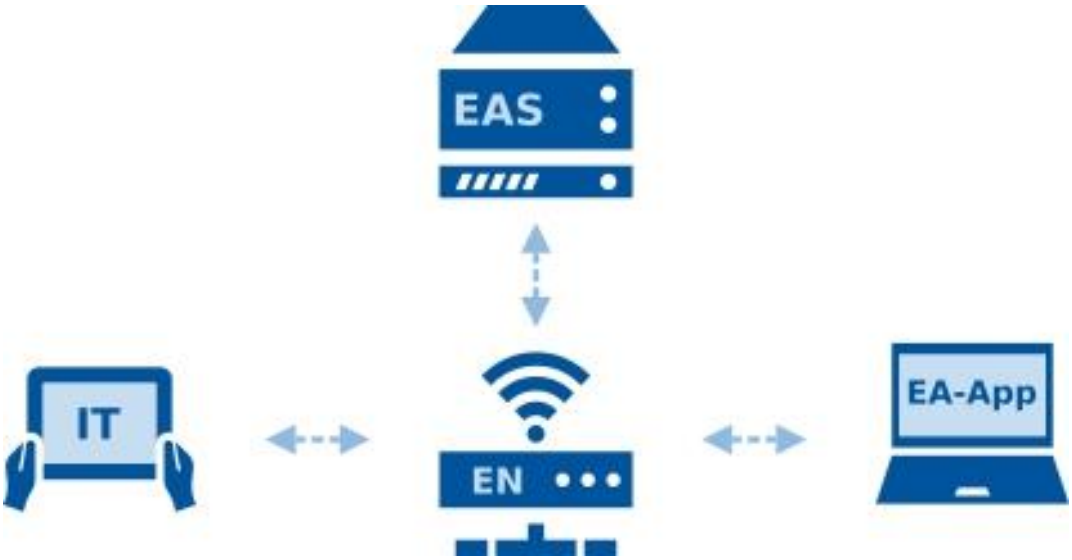

Abb.1 Softwarearchitektur der EA-Software

EA-App

[4] Genauere Angaben zur Evaluation finden sind in [12].

Die EA-App wird auf den Geräten der Studierenden ausgeführt. Sie stellt die grafische Schnittstelle für die Bearbeitung der Klausuraufgaben dar. Zudem bietet sie auch einen Mechanismus, um Prüfungsbetrug auf den Geräten zu identifizieren.

Die EA-App wird im Vollbildmodus gestartet, d. h. sie wird von keinem anderen Fenster überlagert. Sie überwacht vom Start an, ob die Studierenden den Vollbildmodus verlassen oder ob ein Teil oder das gesamte Fenster von einem anderen Fenster überlagert wird. Wenn keine überlappenden Fenster erkannt werden, wurde kein anderes Fenster angezeigt und somit außer der EA-App kein anderes Programm mit einer grafischen Benutzeroberfläche (GUI) verwendet. Wenn Studierende Geräte mit mehr als einem Bildschirm haben, werden alle zusätzlichen Bildschirme mit einem leeren Fenster gefüllt, so dass dort die gleiche Überwachung stattfindet. Darüber hinaus werden Tastatureingaben überprüft, um sicherzustellen, dass sie wirklich von einer Tastatur stammen und nicht von einem anderen Prozess, der Tastatureingaben simuliert, oder von Inhalten, die aus der Zwischenablage eingefügt wurden. Da es gültige Anwendungsfälle für die Zwischenablage gibt, muss eine separate Implementierung der Zwischenablage bereitgestellt werden, die von der EA-App vollständig überwacht wird. Auch die Maus wird überwacht, um sicherzustellen, dass der Mauszeiger nicht von einem Hintergrundprozess verwendet wird, um irgendeine Art von Kommunikation zu ermöglichen.

Der oben beschriebene Ansatz funktioniert jedoch nur, wenn die interne Nachrichtenverarbeitung des Betriebssystems nicht manipuliert wird, denn in diesem Fall könnten die Studierenden verhindern, dass wichtige Ereignisse ausgelöst werden. Es muss also sichergestellt werden, dass die Verarbeitung der notwendigen Ereignisse wie vorgesehen funktioniert.

Die Software ist so konzipiert, dass für die Ausführung der EA-App keine administrativen Rechte auf den Geräten der Studierenden erforderlich sind. Diese Anforderung ist besonders wichtig, da nicht alle Studierenden ein Programm ausführen möchten, das diese Art von Berechtigungen auf ihren Geräten erfordert. Darüber hinaus verwendet die EA-App keine Speichermechanismen des Betriebssystems. Alle Konfigurationen werden in einer lokalen Konfigurationsdatei gespeichert. Dadurch kann die EA-App auf einem System ohne Interaktion mit dem Rest des Betriebssystems, einschließlich des Dateisystems, ausgeführt werden. So kann beispielsweise ein zusätzliches Benutzerkonto eingerichtet werden, das nur Zugriff auf die EA-App und das Zertifikat hat, um zu verhindern, dass die EA-App andere Inhalte des Dateisystems überhaupt lesen kann. Da das Thema Datenschutz sehr wichtig ist, wird der Quellcode der EA-App und des EA-Servers als Open-Source-Projekt veröffentlicht. So können die Studierenden überprüfen, was mit ihrem Zertifikat auf ihrem lokalen Computer und mit ihren Daten auf dem EA-Server geschieht, bevor sie der Nutzung der EA-Software zustimmen.

Der modulare Aufbau der EA-App ermöglicht es, die von Studierenden oder Prüfenden wahrgenommenen Vorteile elektronischer Prüfungen in die EA-App zu integrieren. Im Grunde kann jedes denkbare Feature per Modul in die EA-Anwendung integriert werden. Beispielsweise könnte für eine Prüfung in den Ingenieurswissenschaften oder in der Architektur ein CAD-Tool als Modul integriert werden, so dass die Studierenden dieses Tool aus ihrem späteren Berufsleben direkt in der Prüfung einsetzen können. Damit kann über die Module des Frameworks das von den befragten Studierenden (s.o.) als Vorteil elektronischer Prüfungen benannte realitätsnahe Prüfen realisiert werden.

EA-Server

Der EA-Server stellt den Gegenpart zu EA-App bereit und verwaltet im Hintergrund alle relevanten Daten. Dazu gehören die Anmeldungen zu Klausuren, die Aufgaben einzelner Klausuren oder die

Antworten der Studierenden. Der technische Aufbau wird im Nachfolgenden kurz beschrieben. Dabei wird versucht, nur auf die essenziellen Punkte kurz einzugehen.

Ein *microservice pattern* erlaubt es, die Abhängigkeiten zwischen den verschiedenen Modulen des EA-Servers zu reduzieren. Dies erlaubt die einfache Anpassung der Serverinfrastruktur an spezifische Bedürfnisse einzelner Hochschulen. Diese Modularisierung sollte jedoch nicht die Sicherheit der Serverinfrastruktur gefährden. Der EA-Server besteht daher aus mehreren funktionalen Schichten und einer Proxy-Schicht zum Schutz des Servers vor unbefugtem Zugriff, indem sie die anderen Schichten gegen den Zugriff von außen abkapselt.

Die prozessorientierte Schicht bietet verschiedene Workflows zur Unterstützung der Prüfungsprozesse, wie z.B. das Ablegen einer Prüfung oder die Vorbereitung von Prüfungsfragen. Sie definiert die primäre Schnittstelle für die EA-App. Die persistente Speicherschicht verwaltet Dateisysteme, Datenbanken und Protokolle. Um die Sicherheit zu gewährleisten, greifen alle höheren Schichten auf die Autorisierungs- und Sicherheitsschicht zu, die Informationen über Identitäten und deren Rollen innerhalb der Prozesse sowie Kryptographie- und Signaturfunktionen zur Sicherung der Workflows bereitstellt.

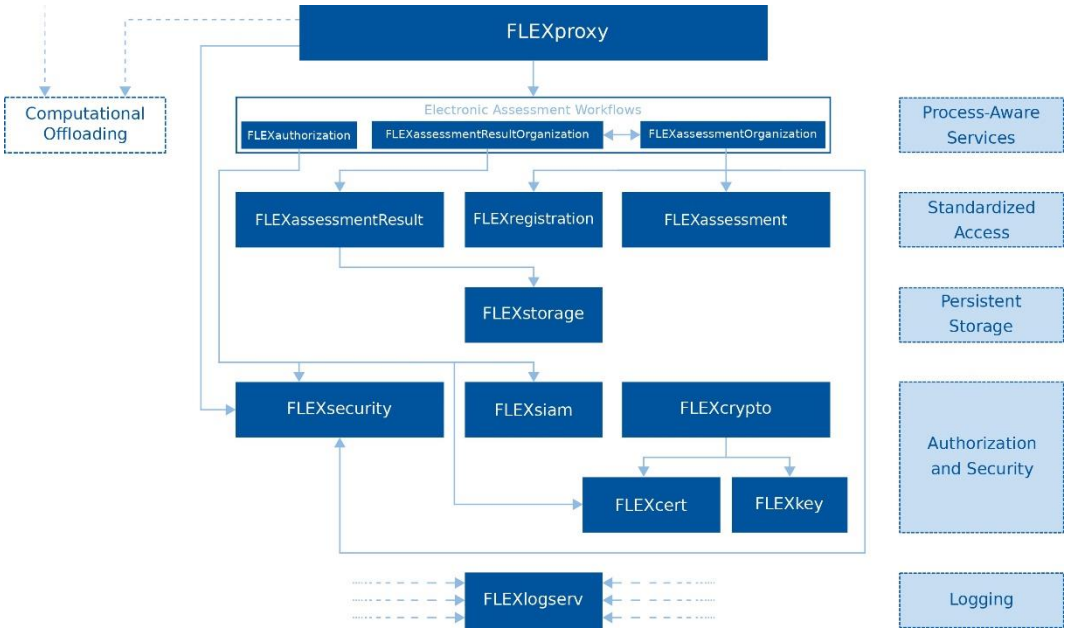

Abb. 2: Architektur des EA-Servers

Wenn ein Microservice auf einer der Schichten eine Logdatei schreiben muss, kann dieser Service auf die Logging-Schicht zurückgreifen, die diese Funktionalität bereitstellt. Um eine klare Trennung der Belange zu erreichen und die Wiederverwendbarkeit der verschiedenen Module in den Schichten zu ermöglichen, hat jedes Modul klar definierte Schnittstellen und Abhängigkeiten. Die Ebenen sind so konzipiert, dass höhere Ebenen nur von Modulen der niedrigeren Ebene abhängen dürfen, aber nicht umgekehrt, um zirkuläre Abhängigkeiten zu vermeiden.

Alle Microservices bieten eine REST-API. Die Endpunkte können potenziell von Studierenden, Prüfer:innen und Mitarbeiter:innen der Organisation genutzt werden. Jeder Endpunkt gibt einen Statuscode 200 für eine gültige Anfrage, einen Statuscode 400 für eine gültige Anfrage mit fehlerhaften Parametern oder einen Statuscode 500 für eine ungültige oder unautorisierte Anfrage zurück.

Die Serverarchitektur von FLEX erlaubt auch **die Bewertung der Ergebnisse von Gruppenarbeiten**. Dies ist durch die Art und Weise möglich, wie die Prüfungsergebnisse vom Microservice FLEXstorage gespeichert werden. Er verwendet ein Git-Backend. Daher werden die Ergebnisse der Studierenden versioniert und bestimmte Änderungen an den Ergebnissen können bestimmten Studierenden zugeordnet werden. Bei individuellen Prüfungen sind die Autor:innen bei jeder Aktualisierung der Ergebnisse auf dem Server dieselben. Bei der Bewertung einer Arbeitsgruppe können die Beiträge zur endgültigen Lösung jedoch verschiedenen Studierenden zugeordnet werden. Das ermöglicht es den Prüfenden, für alle Studierenden eine individuelle Note zu ermitteln, da die individuellen Beiträge zur Lösung unterschieden werden können. Aktualisierungen der Ergebnisse, die von einzelnen Studierenden hochgeladen wurden, können auch von den anderen Studierenden einer Arbeitsgruppe abgerufen werden. Somit wird ein gemeinsames Arbeiten an den Aufgaben einer Prüfung möglich. Zusätzlich verhindert die Speicherung der Ergebnisse in einem versionierten Git-Repository auf dem Server Datenverluste während der Prüfung. Die EA-App implementiert einen Mechanismus, der die Ergebnisse der Studierenden in bestimmten Zeitabständen automatisch auf dem EA-Server speichert. Wenn Geräte von Studierenden während der Prüfung abstürzen, können die bis dahin von den Studierenden hochgeladenen Ergebnisse nach einem Neustart des Geräts problemlos vom Server abgerufen werden.

Um die Manipulation der Prüfungsergebnisse auf dem EA-Server zu verhindern, werden digitale Zertifikate verwendet, um eine Signatur für jeden Satz von Ergebnissen zu erstellen. Daher verwendet die EA-App die privaten Schlüssel der Studierenden, um eine Signatur der Ergebnisse zu erstellen, und lädt diese Signatur zusammen mit den Ergebnissen hoch. Diese Signatur verhindert, dass die Prüfenden die Ergebnisse manipulieren können. Außerdem dürfen die Studierenden nicht in der Lage sein, die Ergebnisse zu manipulieren. Deshalb wird die hochgeladene Signatur mit dem privaten Schlüssel des EA-Servers signiert. Das bedeutet, dass beide Parteien, die EA-App und der EA-Server, den Ergebnissen, die auf den EA-Server hochgeladen wurden, zugestimmt haben. Daher können weder Studierende noch Prüfende einen hochgeladenen Satz von Ergebnissen eigenmächtig ändern, da in diesem Fall die Signatur des anderen Parts fehlen würde.

Die Möglichkeit des *computational offloading* ist wichtig, um Unterschiede zwischen den Geräten der Studierenden auszugleichen. Wie in Abschnitt 5 erörtert wird, hängt die Leistung der EA-App von dem Computer ab, auf dem sie ausgeführt wird, und von der Architektur der EA-App selbst. Es kann jedoch rechenintensive Aufgaben geben, z. B. die Ausführung eines Stücks Quellcode, die auf verschiedenen Geräten zu großen Leistungsunterschieden führen können. Daher können diese rechenintensiven Aufgaben auf den EA-Server verlagert werden. Auf diese Weise sind alle Studierenden bei der Ausführung dieser Aufgaben auf denselben Server angewiesen, was als fair angesehen werden kann. Damit dieser Ansatz wie beabsichtigt funktioniert, ist es jedoch wichtig, die EA-App zumindest für alle gängigen Betriebssysteme verfügbar zu machen. Andernfalls wären die Studierenden benachteiligt, deren Betriebssystem nicht unterstützt wird.

Prüfungsnetzwerk

Die Verbindung zwischen EA-Anwendung und EA-Server wird ¨über ein spezielles Prüfungsnetzwerk (*examination network*, EN) hergestellt. Dieses Netz ist das einzige, über das auf den EA-Server zugegriffen werden kann. Das bedeutet insbesondere, dass ein „reguläres" Netzwerk einer Hochschule, z.B. eduroam, keine Verbindungen zum EA-Server zulassen darf. Während einer elektronischen Prüfung werden die Benutzerkonten der eingeschriebenen Studierenden vom regulären Netz auf das EN übertragen. Daher können sich alle eingeschriebenen Studierenden während der Prüfung nur mit dem EN verbinden, nicht aber mit anderen Netzwerken in der Hochschule. Außerdem können Studierende die EN-Zugangsdaten nur für eine Verbindung verwenden, so dass mehrere Verbindungen mit denselben Zugangsdaten nicht möglich sind. Das Prüfungsnetzwerk verwaltet den Netzwerkverkehr mit einer Firewall und verhindert jegliche Verbindungen zwischen zwei Clients. Es ist jedoch nicht möglich Studierende daran zu hindern, Punkt-zu-Punkt-Verbindungen über Ad-hoc-Wi-Fi-Netze oder sogar mobile Internetverbindungen wie LTE herzustellen. Daher ist dies eine Bedrohung, deren Abwendung in der EA-App implementiert werden muss.

Für die meisten Hochschuleinrichtungen, die bereits ein WLAN-Netzwerk bereitstellen, ist keine zusätzliche Hardware erforderlich, um ein EN einzurichten. Vielmehr kann die bereits vorhandene Hardware genutzt werden, um einen neuen Service Set Identifier (SSID) zu erzeugen, der die Anforderungen des Prüfungsnetzwerkes erfüllt.

Aufsichts-Tablets

Das Aufsichts-Tablet (*invigilator tablet*, IT) wird hauptsächlich als Ersatz für papierbasierte Anmeldelisten verwendet. Es kann die aktuelle Anmeldeliste vom EA-Server herunterladen, so dass die Aufsichtspersonen diese digitale Liste für die Überprüfung der Klausuranmeldungen in ähnlicher Weise wie bei den papierbasierten Prüfungen verwenden können. Die Studierenden können ihre Teilnahme an der Prüfung auf dem Tablet unterschreiben.

Darüber hinaus kann eine valide Verbindung der EA-App zum EA-Server durch Scannen eines QR-Codes überprüfen, der in der EA-App angezeigt wird und Informationen über die Studierenden enthält, wie z. B. den vollständigen Namen und die Version der verwendeten EA-App. Diese Funktion ist wichtig, um Prüfungsbetrug vorzubeugen.

> In einer elektronischen Prüfung wäre **Betrug** möglich, wenn eine andere Person, die nicht im Prüfungsraum anwesend ist, sich mit den Anmeldedaten und dem Zertifikat anderer Studierende beim EA-Server anmelden würde. Allerdings müssten diese Studierenden im Prüfungsraum anwesend sein, damit seine Teilnahme an der Prüfung ordnungsgemäß registriert wird, und die EA-App müsste für die Aufsichtsführenden wie eine unveränderte Version aussehen, die ordnungsgemäß beim EA-Server angemeldet ist.

Jedes aktuelle Tablet sollte als IT genutzt werden können. Da die auf dem IT laufende Anwendung keine rechenintensiven Aufgaben ausführt, sondern nur eine Verwaltungsschnittstelle bietet, die eine Verbindung zum EA-Server herstellt, sind die Anforderungen an die Hardware sehr gering. Allerdings muss das Tablet in der Lage sein, sich mit dem Prüfungsnetzwerk zu verbinden. Daher ist es notwendig, die Hardware-Spezifikationen des Prüfungsnetzes zu beachten. Diese sollten jedoch mit einem neu gekauften Gerät sehr einfach zu erfüllen sein.

5. Organisatorischer Rahmen

Nicht jede Anforderung kann durch das Softwaredesign und die Implementierung der EA-Software erfüllt werden. Daher muss die Erfüllung bestimmter Anforderungen durch eine Reihe von Regeln und Randbedingungen sichergestellt werden.

Studierende und Prüfende müssen in der Lage sein, **FLEX** und alle seine Komponenten zu inspizieren. Für Studierende sind die internen Funktionen der EA-App von besonderer Bedeutung, da dies die Software ist, die sie auf ihren persönlichen Geräten ausführen sollen. Für Prüfende ist es wichtig zu sehen, ob **FLEX** in der Lage ist, ihre Anforderungen für Prüfungen zu erfüllen.

Alle Daten, seien es die Ergebnisse der Studierenden oder die Aufgaben einer Prüfung, müssen verlustsicher gespeichert werden. Da bei einem Dateispeichersystem nicht garantiert werden kann, dass es ordnungsgemäß funktioniert, muss dies durch Backups erreicht werden. Hierfür könnte z.B. ein Bandsystem [26] verwendet werden, da dieses die sehr ähnlichen Anforderungen eines Forschungsdatenmanagementsystems [27] erfüllt.

Allerdings reicht es nicht aus, Zertifikate auszustellen, die nur im Rahmen von elektronischen Prüfungen gültig sind. Vielmehr muss die Nutzung von Zertifikaten zur Identifikation von Studierenden in einem digitalen Prozess für den gesamten (digitalen) Lebenszyklus von Studierenden umgesetzt werden. Dies ist so, da Zertifikate, die nur für einen einzelnen Anwendungsfall genutzt werden, keinen inhärenten Wert haben. Das ist vergleichbar mit einem Schlüssel, der nur eine einzige Tür in einem Haus aufschließen kann. Dieser Schlüssel selbst hat maximal den Gegenwert des Rauminhalts. Ein Zertifikat für den gesamten digitalen Lebenszyklus von Studierenden ist aber vergleichbar mit einem Generalschlüssel für alle Türen des Hauses. Dieser hat einen viel höheren Wert, sodass er nicht ohne Weiteres weitergegeben wird.

Obwohl die meisten Studierenden über die für die Durchführung von elektronischen Prüfungen geeignete Geräte verfügen, haben einige Studierende möglicherweise keinen Zugang zu einem solchen Gerät. Um diesen Studierenden die Teilnahme an einer elektronischen Prüfung zu ermöglichen, muss die Hochschule Leihgeräte zur Verfügung stellen. Diese Studierenden, aber auch Studierende, die zwar über ein eigenes Gerät, aber nicht ausgeprägte Computerkenntnisse verfügen, können auf Probleme stoßen, wenn es um digitale Zertifikate und portable Anwendungen geht. Daher muss die Hochschule auch technische Unterstützung leisten.

6. Ausblick

Selbst wenn ein funktionsfähiger Prototyp zur Verfügung steht, der die gesammelten Anforderungen erfüllt, ist das Projekt noch nicht abgeschlossen. Mit einer flexiblen Softwarelösung an der Hand, verlagert sich der Fokus auf die praktische Anwendung der Software. Im September 2020 wurde ein Feldtest im Rahmen des MATSE-Ausbildungsprogramms mit etwa 200 Auszubildenen durchgeführt. Seitdem wurde FLEX regelmäßig für die Durchführung elektronischer Modulprüfungen im Java-Modul des Studiengangs verwendet.

Um den Einsatz von FLEX auch für andere Hochschulen attraktiv zu machen, hat es sich als wichtig erwiesen, die Verwendung anderer digitaler Werkzeuge mit FLEX zu ermöglichen, z.B. ein LMS für die

Erstellung von Prüfungen. Darüber hinaus ist die Unterstützung eines breiteren Spektrums mobiler Geräte wie Tablet-Computer und vielleicht sogar Smartphones geplant. Es ist unbestreitbar, dass diese Geräte nicht für jede Art von Prüfung geeignet sind, für die ein Notebook geeignet ist; es gibt jedoch Aufgabentypen, z. B. Multiple-Choice-Aufgaben, die mit solchen Geräten gelöst werden können. Bei der Portierung von FLEX auf mobile Betriebssysteme wie Android und iOS ist von vornherein klar, dass nicht alle implementierten Anti-Betrugs-Maßnahmen auf diesen Plattformen funktionieren werden. Daher muss ein erheblicher Arbeitsaufwand betrieben werden, um die speziellen Anforderungen von Anti-Betrugs-Maßnahmen auf mobilen Plattformen zu lösen.

Jenseits der praktischen Anwendung und mit einem viel stärkeren Fokus auf die Forschung werden die Möglichkeiten, die eine Software wie FLEX bietet, evaluiert. Von besonderem Interesse ist dabei die automatische Korrektur von Programmieraufgaben und die Integration solcher Mechanismen in FLEX. Darüber hinaus sind **neue Arten von Aufgabenstellungen** von Interesse. Für Softwareentwickler:innen ist es eigentlich kein übliches Szenario, eine sehr begrenzte Aufgabe ohne technische Hilfsmittel zu entwickeln. Vielmehr ist die Entwicklung von komplexeren Aufgaben in einem Entwicklungsteam die Realität im Arbeitsalltag. Daher ist die Integration von Teamarbeit in eine Prüfung bei gleichzeitiger Beibehaltung der Möglichkeit, Studierende individuelle Noten zu geben, ein weiteres interessantes Thema für eine zukunftsgerichtete Prüfungskultur.

Ein drittes interessantes Thema ist die **Barrierefreiheit**. Technologie ist eine Möglichkeit, bestimmte Einschränkungen einer Behinderung im Allgemeinen zu überwinden und dasselbe gilt für den Bereich der Bildung [28]. Daher eröffnet ein EA-Framework die Möglichkeit, die Fähigkeit zur Ablegung von Prüfungen für behinderte Studierende in einer Weise zu verbessern, wie es bei einer papierbasierten Prüfung niemals möglich wäre.

Literatur

1. E. Dahlstrom, C. Brooks, S. Grajek, and J. Reeves, Undergraduate Students and IT, Louisville, 2015. https://library.educause.edu/%7E/media/files/library/2015/8/ers1510ss.pdf?la=en (11.07.2023)
2. H. Poll, Student Mobile Device Survey 2015: National Report: College Students, 2015. https://www.pearson.com/content/dam/one-dot-com/one-dot-com/ped-blogs/wp-content/pdfs/2015-Pearson-Student-Mobile-Device-Survey-College.pdf (11.07.2023)
3. J. Willige, Auslandsmobilität und digitale Medien: Arbeitspapier Nr. 23, Geschäftsstelle Hochschulforum Digitalisierung beim Stifterverband für die Deutsche Wissenschaft e.V, Ed., Berlin, 2016. https://hochschulforumdigitalisierung.de/sites/default/files/dateien/HFD_AP_Nr23_Digitale_Medien_und_Mobilitaet.pdf
4. Fluck and M. Hillier, "eExams: Strength in diversity," in IFIP Advances in Information and-Communication Technology, Springer International Publishing, 2017, pp. 409–417. DOI: 10.1007/978-3-319-74310-3 42
5. I. Melve. (2013). BYOD for exams: leaving students to their own devices, https://de.slideshare.net/imelve/tnc-melve20130605v04 (11.07.2023)
6. B. Küppers, T. Eifert, M. Politze, and U. Schroeder, "e-Assessment Behind the Scenes, Common Perceptions of e-Assessment and How We See It Nowadays," in Proceedings of the 10th International Conference on Computer Supported Education - Volume 2, CSEDU 2018 - 10th International Conference on Computer Supported Education, Funchal, Madeira (Portugal), 15. Mar 2018 - 17. Mar 2018, SciTePress, 2018, pp. 285–291, DOI: 10.5220/0006788402850291
7. B. Küppers and U. Schroeder, "Bring Your Own device for e-Assessment, A Review," in EduLearn 16: 8th International Conference on Education and New Learning Technologies, L. Gòmez Chova, A. Lòpez Martinez, and I. Candel Torres, Eds., EDULEARN 2016 - 8th International Conference on Education and New Learning Technologies, Barcelona (Spain), 4. Jul 2016 - 6. Jul 2016, Valencia: IATED Academy, 2016, pp. 8770–8776. DOI: 10.21125/edulearn.2016.0919
8. B. Küppers and U. Schroeder, "A Framework for e-Assessment on Students' Devices, Technical Considerations," in Technology Enhanced Assessment, E. Ras and A. E. Guerrero Roldàn, Eds., ser. Communications in Computer and Information Science, TEA 2017 - 20th International Conference, Barcelona (Spain), 5. Oct - 6. Oct 2017, vol. 829, Cham: Springer International Publishing, 2018, pp. 83–95. DOI: 10.1007/978-3-319-97807-9 7.
9. V. Terzis and A. A. Economides, "The acceptance and use of computer based assessment," Computers & Education, vol. 56, no. 4, pp. 1032–1044, 2011. DOI: 10.1016/j.compedu.2010.11.017
10. V. Lukarov, "Scaling up Learning Analytics in Blended Learning Szenarien," Dissertation, RWTH Aachen University, Aachen, 2019. DOI: 10.18154/rwth-2019-05165

11. B. Küppers, T. Dondorf, B.Willemsen, H. J. Pflug, C. Vonhasselt, B. Magrean, M. S. Müller, and C. Bischof, "The Scientific Programming Integrated Degree Program – A Pioneering Approach to Join Theory and Practice," Procedia Computer Science, vol. 80, pp. 1957–1967, 2016. DOI: 10.1016/j.procs.2016.05.516

12. B. Küppers, U. Schroeder, "FLEX: A BYOD Approach to Electronic Examinations," in Babo, R., Dey, N., Ashour, A.S. (eds), Workgroups eAssessment: Planning, Implementing and Analysing Frameworks (Springer ISRL, vol 199) pp. 145-179, 2020. DOI: 10.1007/978-981-15-9908-8_6

13. S. Kocdar, A. Karadeniz, R. Peytcheva-Forsyth, and V. Stoeva, "Cheating and plagiarism in e-assessment: Students' perspectives," Open Praxis, vol. 10, no. 3, p. 221, 2018. DOI: 10.5944/openpraxis.10.3.873

14. M. Hillier, S. Grant, and M. A. Coleman, "Towards authentic e-Exams at scale: robust networked Moodle," in ASCILITE 2018 - Conference Proceedings, M. Campbell, J.Willems, C. Adachi, D. Blake, I. Doherty, S. Krishnan, S. Macfarlane, L. Ngo, M. O'Donnell, S. Palmer, L. Riddell, I. Story, H. Suri, and J. Tai, Eds., ASCILITE 2018, Geelong (Australia), 25. Nov 2018 - 28. Nov 2018, vol. 35, 2018, pp. 131–141. https://2018conference.ascilite.org/wp-content/uploads/2018/12/ASCILITE-2018-Proceedings-Final.pdf (11.07.2023)

15. C. Rolim and P. Isaias, "Examining the use of e-assessment in higher education: Teachers and students' viewpoints," British Journal of Educational Technology, no. 4, pp. 1785–1800, 2018. DOI: 10.1111/bjet.12669

16. H. Mellar, R. Peytcheva-Forsyth, S.Kocdar, A. Karadeniz, and B.Yovkova, "Addressing cheating in e-assessment using student authentication and authorship checking systems: teachers' perspectives," International Journal for Educational Integrity, vol. 14, no. 1, p. 2, 2018, DOI: 10.1007/s40979-018-0025-x

17. M. Jamil, R. H. Tariq, and P. A. Shami, "Students' Perceptions to Use Technology for Learning: Measurement Integrity of the Modified Fennema-Sherman Attitudes Scales," Turkish Online Journal of Educational Technology-TOJET, vol. 11, no. 4, pp. 371–381, 2012.

18. M.Kuikka, M. Kitola and M.-J. Laakso, "Challenges when introducing electronic exam", Research in Learning Technology, vol. 22, 2014. DOI: 0.3402/rlt.v22.22817

19. H. Nacken and C. Knight. (2019). Digitalization Strategy for Teaching, http://www.rwth-aachen.de/cms/%7Ehjfu/?lidx=1 (11.07.2023)

20. RWTH Aachen University. (2018). Digitalisierungsstrategie der Lehre an der RWTH Aachen - Die zweite Phase 2018 – 2023. https://www.rwth-aachen.de/global/show_document.asp?id=aaaaaaaaaayitvk (11.07.2023)

21. S. Glaser. (2015). Ordnung zum Schutz personenbezogener Daten bei multimedialer Nutzung von E-Learning-Verfahren an der Rheinisch-Westfälischen Technischen Hochschule Aachen https://www.rwth-aachen.de/global/show_document.asp?id=aaaaaaaaaaolwek (11.07.2023)

22. J. Sheard, S. Markham, and M. Dick, "Investigating Differences in Cheating Behaviours of IT Undergraduate and Graduate Students: The maturity and motivation factors," Higher Education Research & Development, vol. 22, no. 1, pp. 91–108, 2003. DOI: 10.1080/0729436032000056526

23. G. Sindre and A. Vegendla. (2015). E-exams versus paper exams: A comparative analysis of cheating-related security threats and countermeasures. https://scholar.google.com/citations?view_op=view_citation&hl=en&user=RgHhQKwAAAAJ&citation_for_view=RgHhQKwAAAAJ:9yKSN-GCB0IC (11.07.2023)

24. Akherfi, M. Gerndt, and H. Harroud, "Mobile cloud computing for computation offloading: Issues and challenges," Applied Computing and Informatics, vol. 14, no. 1, pp. 1–16, 2018. DOI: 10.1016/j.aci.2016.11.002

25. D. Kovachev and R. Klamma, "Framework for Computation Offloading in Mobile Cloud Computing," International Journal of Interactive Multimedia and Artificial Intelligence, vol. 1, no. 7, p. 6, 2012. DOI: 10.9781/ijimai.2012.171

26. D. Stanek and T. Eifert, "Maßnahmen für verlässliche und schnelle Datenwiederherstellung," PIK - Praxis der Informationsverarbeitung und Kommunikation, vol. 35, no. 3, 2012. DOI: 10.1515/pik-2012-0032

27. T. Eifert, U. Schilling, H. - J. Bauer, F. Krämer, and A. Lopez, "Infrastructure for Research Data Management as a Cross-University Project," in Human Interface and the Management of Information: Supporting Learning, Decision-Making and Collaboration, Springer International Publishing, 2017, pp. 493–502. DOI: 10.1007/978-3-319-58524-6 39

28. D. L. Edyburn, "Assistive technology and students with mild disabilities," Focus on Exceptional Children, vol. 32, no. 9, 2017. DOI: 10.17161/fec.v32i9.6776

Impressum

Diskussionspapiere des HFD spiegeln die Meinung der jeweiligen Autor:innen wider.
Das HFD macht sich die in diesem Papier getätigten Aussagen daher nicht zu Eigen.

ISSN (Online) 2365-7081; 9. Jahrgang

Zitierhinweis
Küppers, B. (2023). Digitale Prüfungen mit Bring Your Own Device (BYOD). Diskussionspapier Nr. 24. Berlin: Hochschulforum Digitalisierung.

Herausgeber
Geschäftsstelle Hochschulforum Digitalisierung beim Stifterverband für die Deutsche Wissenschaft e.V.
Hauptstadtbüro • Pariser Platz 6 • 10117 Berlin • T 030 322982-520
info@hochschulforumdigitalisierung.de

Redaktion
Jannica Budde

Verlag
Edition Stifterverband – Verwaltungsgesellschaft für Wissenschaftspflege mbH
Barkhovenallee 1 • 45239 Essen • T 0201 8401-0 • mail@stifterverband.de

Layout
Satz: Jannica Budde/Michael Siegel
Vorlage: TAU GmbH • Köpenicker Straße 154a • 10997 Berlin

Das Hochschulforum Digitalisierung ist ein gemeinsames Projekt des Stifterverbandes, des CHE Centrums für Hochschulentwicklung und der Hochschulrektorenkonferenz. Förderer ist das Bundesministerium für Bildung und Forschung.

www.hochschulforumdigitalisierung.de

STIFTERVERBAND
CHE Centrum für Hochschulentwicklung
HRK Hochschulrektorenkonferenz
GEFÖRDERT VOM Bundesministerium für Bildung und Forschung