


**Vergabe eines neuen Passwords an nicht vor Ort anwesende Personen oder auch das Problem der remote Authentifizierung**

**Ergebnisse einer Umfrage unter ZKI-Mitgliedseinrichtungen**

**Hansjörg Ast**  
Goethe Universität



www.goethe-universitaet.de

---

---

---


---

---

---

---

---




From: [fifi-hase@hotmail.com](mailto:fifi-hase@hotmail.com)  
 To: [useradmin@rz.uni-frankfurt.de](mailto:useradmin@rz.uni-frankfurt.de)

Liebes Nutzerbüro,  
 Ich habe mein Password vergessen und muss mich dringend für die Lehrveranstaltungen des kommenden Semesters anmelden. ✓

Leider kann ich nicht persönlich bei Ihnen vorbeikommen, da ich mich noch im Auslandssemester in den USA befinde. ✓

Bitte sendet mir ein neues Password zu. ✗

Liebe Grüße Eure  
 Erika Musterfrau



www.goethe-universitaet.de

---

---

---


---

---

---

---

---




Wie können wir überprüfen, ob Erika Musterfrau die Absenderin der Mail ist und diese Erika Musterfrau die Studierende gleichen Namens mit dem Account **emuster** ist ?

Wie kann sich Frau Musterfrau uns gegenüber remote authentifizieren ?

Wie können wir einen hinreichend sicheren Kommunikationskanal aufbauen ?

Ich habe auf diese Anfrage 17 Antworten erhalten

**Herzlichen Dank für Eure/Ihre Mühe**



www.goethe-universitaet.de

---

---

---


---

---

---


---

---



**HRZ**

**Antworten:**



www.goethe-universitaet.de

Ist nicht möglich, Person muss sich vor Ort authentifizieren

**Bewertung**

- Rechtlich absolut korrekt
- Wird als wenig servicefreundlich empfunden.
- Rechtliche Bedenken werden oft nicht akzeptiert

Missbrauchspotential: **keines**

4

---

---

---


---

---


---

---

---



**HRZ**



www.goethe-universitaet.de

- Versand des neuen Passwords an eine früher eingerichtete Versandt-Adresse (e-mail) – Einrichtung nur mit Authentifizierung möglich.
- SMS an eine vorher hinterlegte Mobilfunknummer – Einrichtung nur mit Authentifizierung möglich.

**Bewertung**

- Entspricht gängiger Praxis vieler Web-Dienste
- Klarschrift Versand des Passwords in der e-mail , ggf. Zusendung eines Einmalpasswords
- Echtheit der Herkunft der Anfrage kann nicht überprüft werden.

Missbrauchspotential: **Gering-Mittel**

dritte Person kann Account nicht kompromittieren, aber ggf. lahm legen

Konsequenzen bei terminkritischen Anwendungen (Windhundverfahren od. Prüfungsanmeldung) sind möglich

5

---

---

---


---

---


---

---

---



**HRZ**



www.goethe-universitaet.de

- Richtige Beantwortung einer/mehrerer vorher hinterlegter Fragen (challenge-response) – Zusendung des neuen Passwords bei e-mail oder SMS

**Bewertung:**

- Antworten dürfen nicht trivial zu erraten sein, oder sich aus persönlichen Gegenständen nicht leicht erschließen lassen – z.b. Geburtsdatum oder Wohnadresse – solche Angaben können sich missliebige KommilitonInnen oder Taschendiebe leicht verschaffen. Überprüfung der Qualität der Fragen bei Hinterlegung?

Missbrauchspotential: **Gering bis Mittel, abhängig von Anzahl und Qualität der Fragen**

Hinreichender? Check der Identität wird so erreicht. Bei e-mail Versandt erfolgt weiterhin eine nicht verschlüsselte Übertragung

6

---

---

---

---

---

---

---

---

**HRZ**

GOETHE UNIVERSITÄT  
FRANKFURT AM MAIN

- Kommunikation über zertifizierte und ggf. verschlüsselte Kanäle

Bewertung:

- rechtlich korrekt, kein Missbrauchspotential bei bestimmungsgemäßer Anwendung**
- Erfordert eigene CA mit PKI Ausgabe oder Zuordnung des public keys des Bundespersonalausweises zum Studierenden
- Kryptokarten sind teuer
- Handhabung kompliziert – erfordert u.a. die Mitführung eines Lesegeräts
- Überfordert aktuell die meisten unserer Kunden – würde deshalb als wenig Servicefreundlich empfunden
- Mir ist aktuell niemand bekannt, der es wirklich anwendet

www.goethe-universitaet.de

7

---

---

---

---

---

---

---

---

**HRZ**

**eKaay Verfahren**

GOETHE UNIVERSITÄT  
FRANKFURT AM MAIN

Wilhelm-Schickard-Institut für Informatik Universität Tübingen

Authentifizierung und login per Smartphone

Voraussetzungen:

- Smartphone mit Android oder iOS Betriebssystem und Download einer (kostenfreien) App
- Registrierung des eigenen Handys auf einer Webseite mit klassischer Authentifizierung durch abschnappen eines 2d Codes und Versand dieses Codes via App an den Server



www.goethe-universitaet.de

8

---

---

---

---

---

---

---

---

**HRZ**


GOETHE UNIVERSITÄT  
FRANKFURT AM MAIN

Anwendung:

Aufruf einer Webseite, abschnappen des dort angezeigten Codes und Versand per App an den Server.

Authentifizierung erfolgt und Webseite öffnet sich

Seit Mai 2011 im produktiven Betrieb



www.goethe-universitaet.de

9

---

---

---

---


---

---

---

---

## HRZ



GOETHE  
UNIVERSITÄT  
FRANKFURT AM MAIN

Bewertung: aus meiner Sicht **sicher**, uns ist bislang keine Schwachstelle des Verfahrens aufgefallen

- App kann mit einer unabhörbaren PIN gesichert werden – Schutz bei Diebstahl – sollte m.E. Pflicht werden.
- Kein Angriffspunkt durch key-logger etc. auf einem nicht vertrauenswürdigen Rechner.
- Keine zusätzlichen Werkzeuge notwendig, die der Nutzer nicht sowieso bei sich hat.

Vorteil: Verfahren erscheint „trendy“, hohe Akzeptanz zu erwarten.

Nachteil: Verbreitung von entsprechenden Handys erst bei 15 %, Tendenz aber stark steigend.

Direkte Nutzung ist auf Web-Services beschränkt, aber eine „neues Password“-Seite ist trivial möglich.

www.goethe-universitaet.de
10

---

---

---

---

---

---

---

---

## HRZ



GOETHE  
UNIVERSITÄT  
FRANKFURT AM MAIN

Weitere Infos zum eKaay Verfahren

[www.ekaay.com](http://www.ekaay.com)

Bernd Borchert, WSI Uni Tübingen

[borchert@informatik.uni-tuebingen.de](mailto:borchert@informatik.uni-tuebingen.de)

Aktuell auf der Cebit am Gemeinschaftsstand des BMWi

www.goethe-universitaet.de
11

---

---

---

---

---

---

---

---