RUHR-UNIVERSITÄT BOCHUM

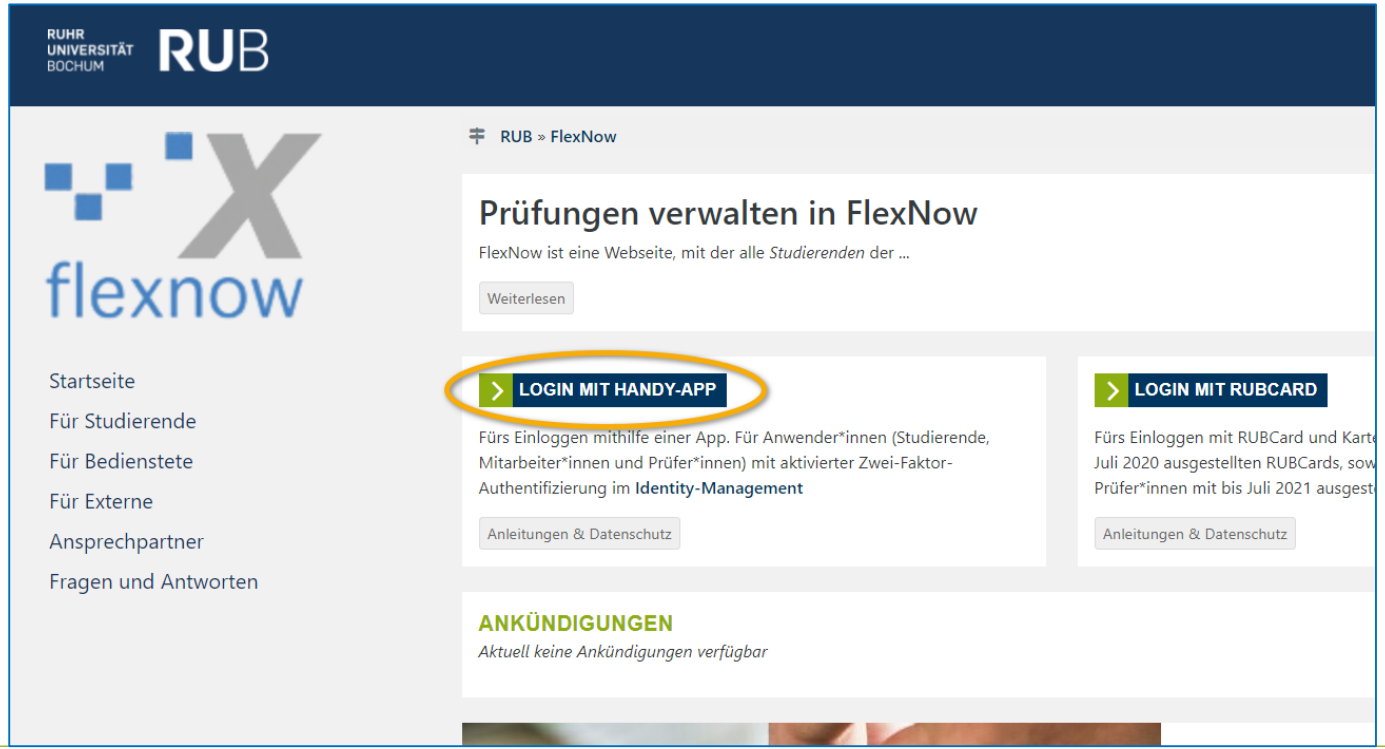
Zwei-Faktor-Authentifizierung fürs FlexNow-Web mit TOTP

Bericht von Peter Fasching, für die FlexNow-Usergroup 28.-29.03.2022

Ablauf beim Einloggen mit „TOTP“

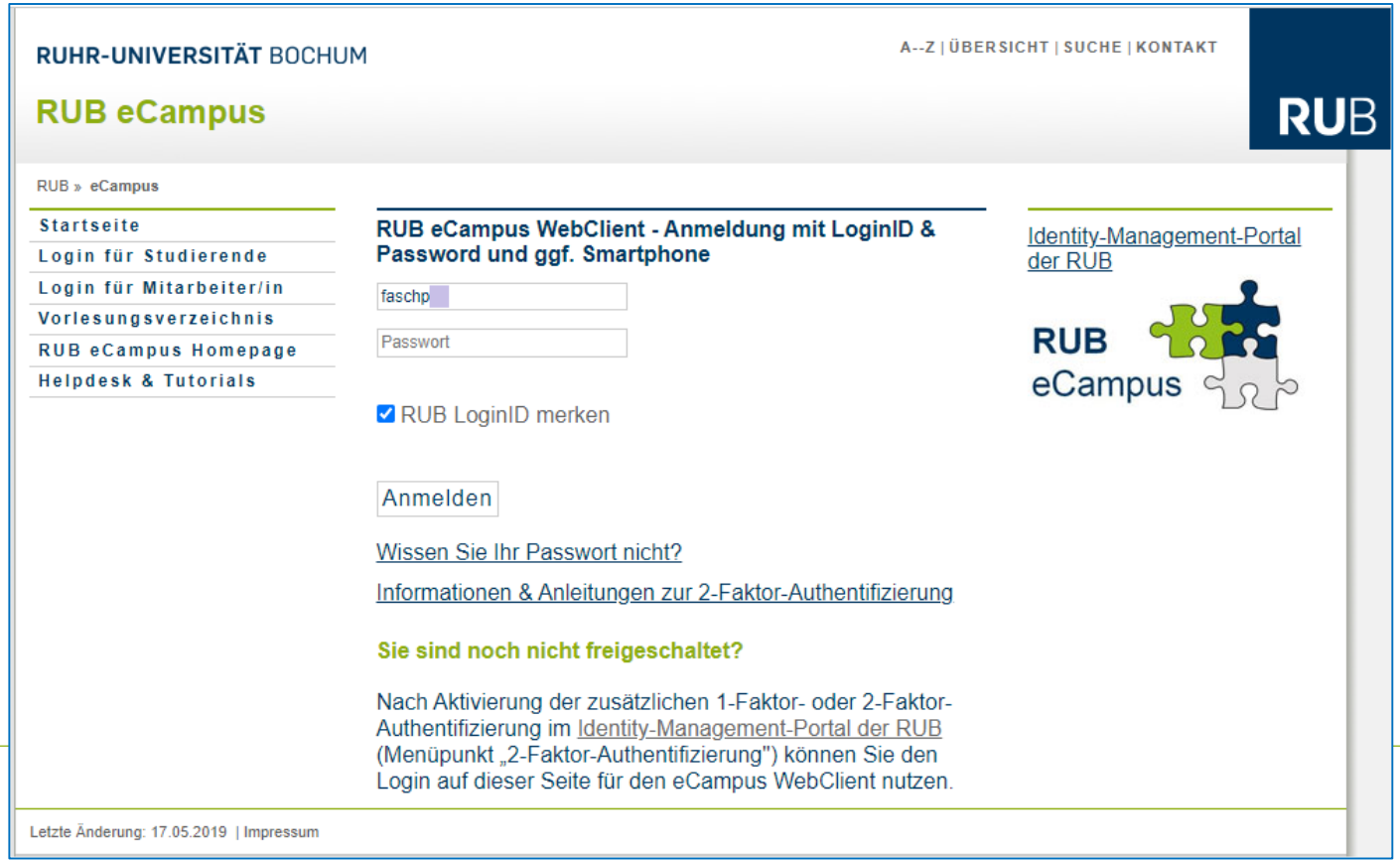
Ablauf beim Einloggen mit „TOTP“:

1.) Login-Button auf unserer Homepage



Ablauf beim Einloggen mit „TOTP“:

2.) Mit RUB-Login-Daten einloggen



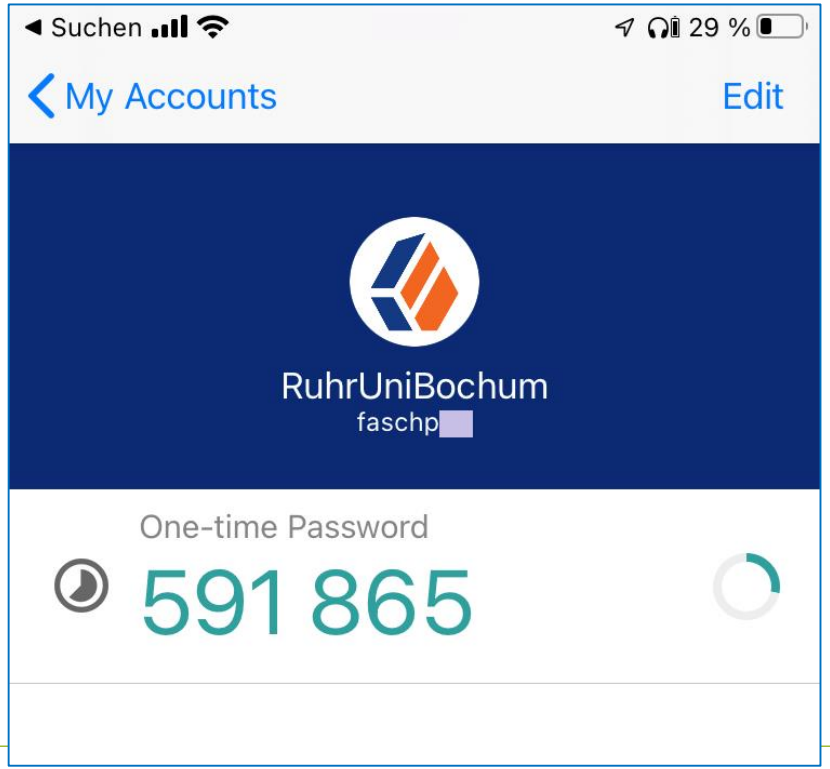
Ablauf beim Einloggen mit „TOTP“:

3.) Mit RUB-Login-Daten einloggen

RUHR UNIVERSITÄT BOCHUM RUB

Ablauf beim Einloggen mit „TOTP“:

4.) Sicherheitscode in ForgeRock-App anzeigen lassen



Das Passwort ändert sich alle 30 Sekunden

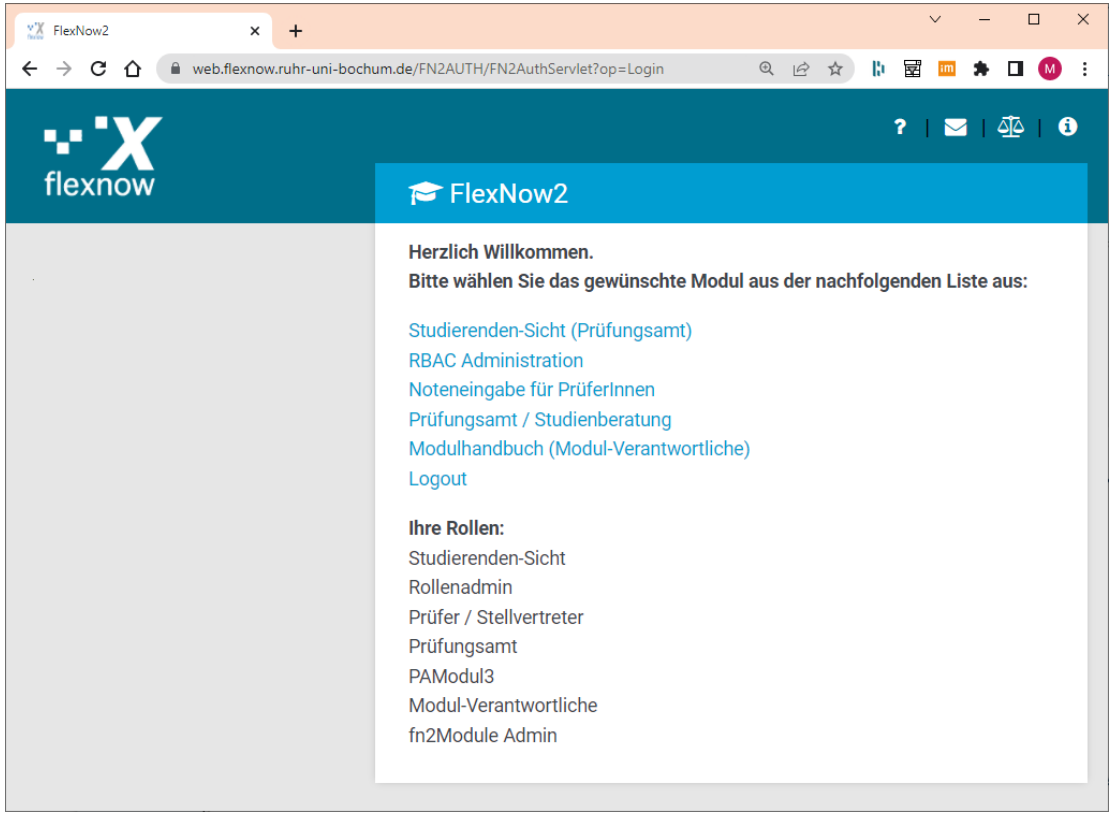
Ablauf beim Einloggen mit „TOTP“:

5.) Sicherheitscode in RUB-Login-Seite

RUHR UNIVERSITÄT BOCHUM RUB

Ablauf beim Einloggen mit „TOTP“:

6.) Fertig – sind im fn2Web



Grundsätzliches zu TOTP

Grundsätzliches zu TOTP

- TOTP: „Time-based One-time Password“ Algorithmus/Verfahren
- TOTP ist ein Verfahren zur Zwei-Faktor-Authentifizierung („2FA“)
- 2FA ist seit Anfang von FlexNow ein Muss in der RUB
- Ab 2020 wird TOTP als zweites Verfahren zur 2FA verwendet
- Funktioniert mit allen nicht ganz alten Smartphones und Tablets

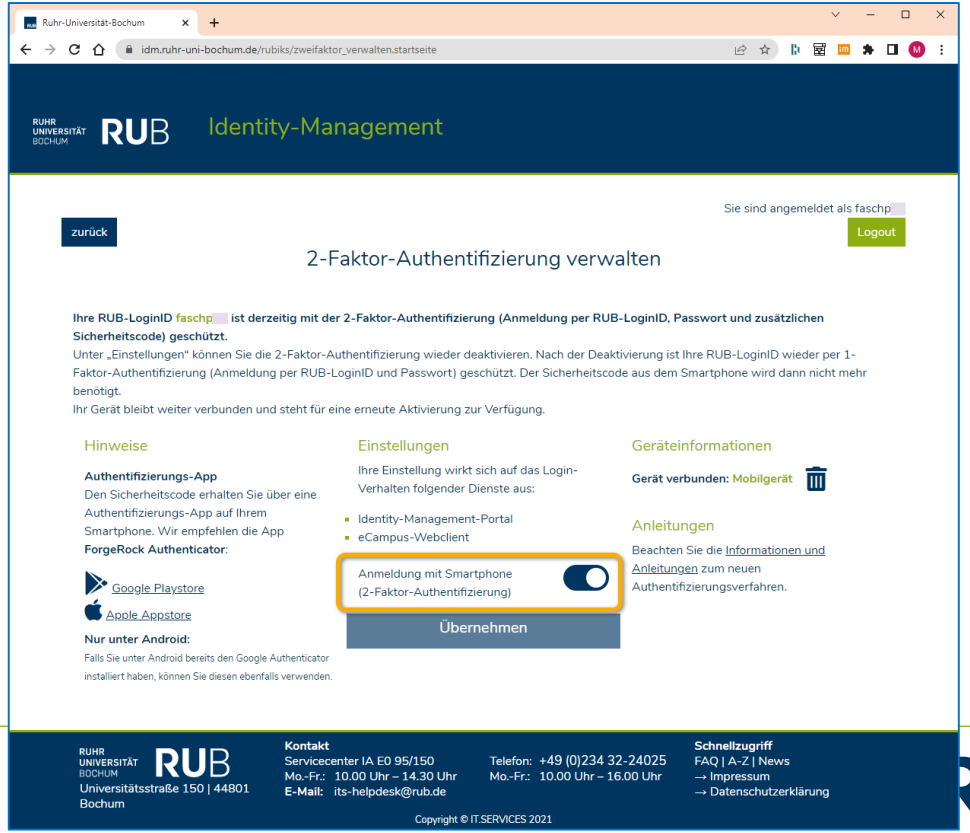
- Frage an Sie: Was sind die beiden Sicherheitsfaktoren bei TOTP?
- Antwort:
  1) Das Passwort des RUB-Logins als erster Faktor („Wissen“)
  2) Der Sicherheitscode als zweiter Faktor („Besitz“ der App auf Handy)

  Nicht verwendet wird also der dritte Faktor „Biometrie“ (z.B. Fingerabdrucksensor)

Vorbereitungen für TOTP von Anwender*innen

Vorbereitungen für TOTP von Anwender*innen

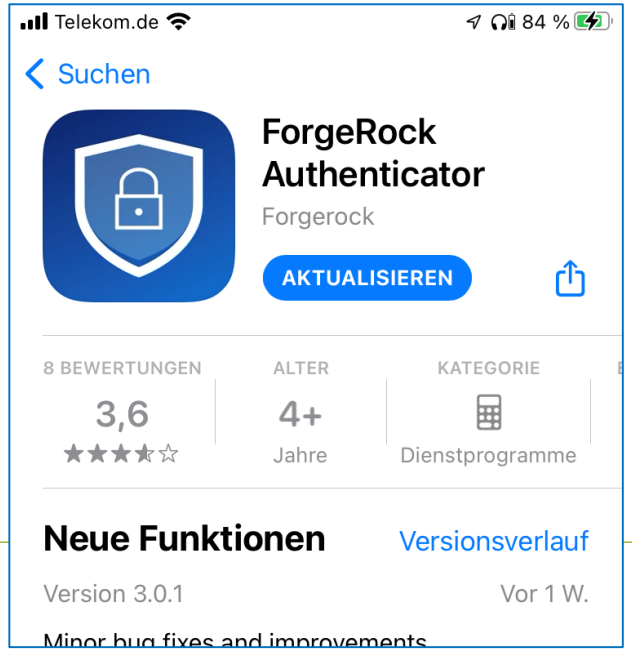
1) Die Zwei-Faktor-Authentifizierung auf einer RUB-Webseite aktivieren, diese zeigt dann einen QR-Code an



Vorbereitungen für TOTP von Anwender*innen

2) Vorbereitung des Smartphones für die Authentifizierung:

- App installieren („ForgeRock Authenticator“, siehe den linken Screenshot, oder bei Android den „Google Authenticator“)
- QR-Code mit App einscannen (rechts)



Vorbereitungen für TOTP
von Admins und IT-Support

Technische Vorbereitungen unseres IT-Dienstleisters

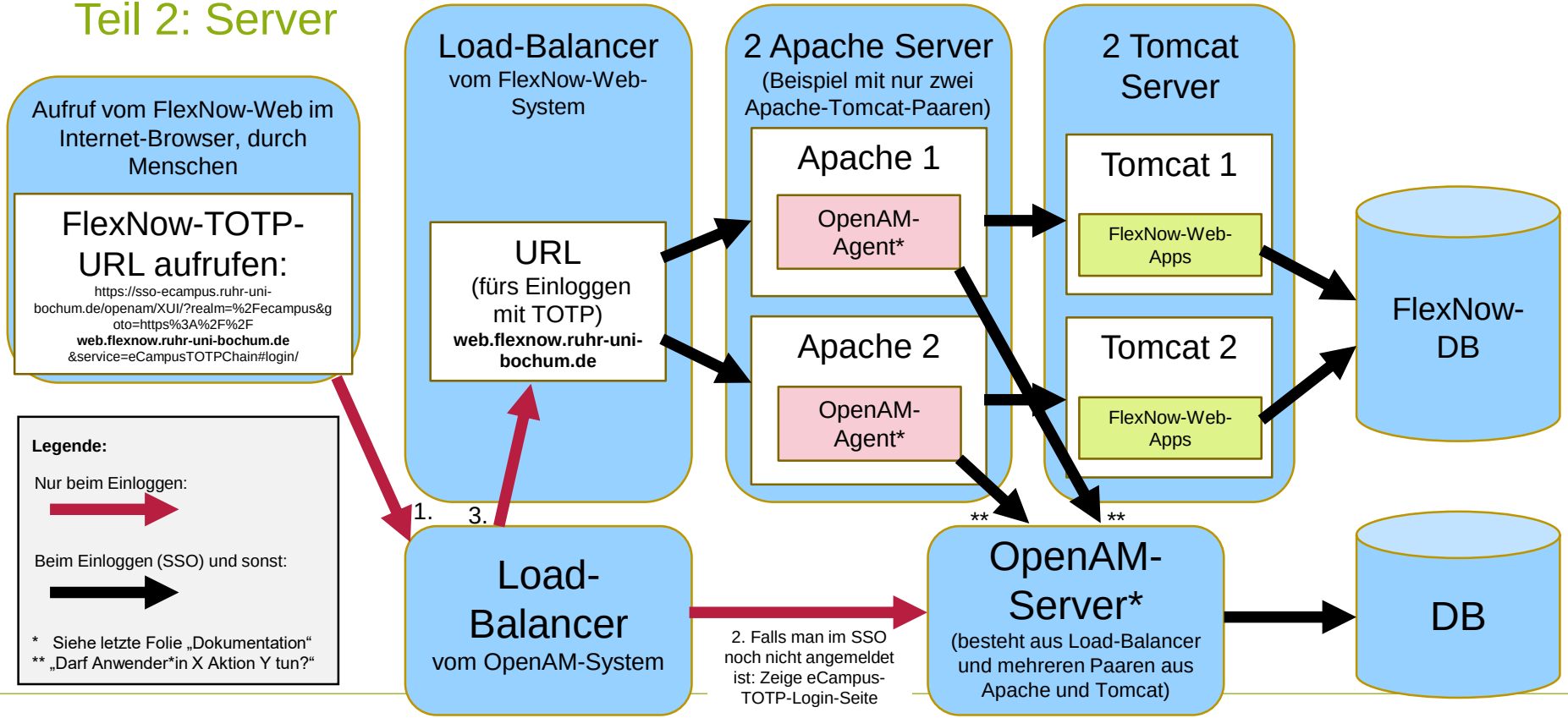
Teil 1: Webseiten und http

- Der „OpenAM-Agent“ muss einen http-Header mit bestimmten Daten ans fn2Web übergeben, siehe den Beschreibung unseres Tickets zur Einführung von TOTP: https://tickets.ihb-eg.de/issues/4883
- Eine Webseite zur Aktivierung der Zwei-Faktor-Authentifizierung (siehe Folie 12) und zum Anzeigen des QR-Codes (Folie 13), alles nach Einloggen mit RUB-Login-Daten
- Eine Webseite zum Einloggen mit den RUB-Login-Daten (Folien 4,5 und 7), die nach fn2Web weiterleitet

RUHR UNIVERSITÄT BOCHUM RUB

Technische Vorbereitungen unseres IT-Dienstleisters

Teil 2: Server



RUHR UNIVERSITÄT BOCHUM RUB

Technische Vorbereitungen von uns als Admins

- In Datenbank neuer **`AuthTyp`** (11) für TOTP:

```
INSERT INTO fn2meta.AuthTyp (authTypId, bez, def, aufruf, verzeichnis, aktiv)
VALUES (11, 'TOTP', 1, null, null, 1);
```

- Zusätzliche **`fn2meta.Auth`**-Einträge durch SOS-Import für jeden Studi automatisch anlegen lassen, zusätzlich zum bisherigen **`AuthTyp`** 8 für „Zertifikat auf Chip-Karte“:

```
INSERT INTO flexnow.Setup_ (param_, value_, locked)
VALUES ('SCHNITTSTELLE_FN2META_AUTHTYPID', '8;11', null);
```

- Prüfen, ob so gesetzt:

```
INSERT INTO flexnow.Setup_ (param_, value_, locked)
VALUES ('DRUCK_FN2AUTH', 'FN2AUTH/FN2AuthServlet?authtyp=1', null);
```

- Eventuell muss die Datei **`custvalues.js`** manuell in /FN2AUTH/js/ abgelegt werden
- Ansprechpartnerin vom ihb war für uns Gerlinde, sie kennt diese technischen Details

Hardware-Token als Alternative zur Handy-App

„Hardware-Token“ vom IT-Dienstleister, statt App

Fakultäten übernehmen für Mitarbeiter*innen die Kosten. Siehe Folie „Dokumentation“, dort „Zwei Dokus von uns“, darin Abschnitt 2.D.b) im „Troubleshooting-Dokument“

Vorteile / Nachteile

Vor- und Nachteile von TOTP

Vorteile von TOTP:

- Mehr Datensicherheit durch Zwei-Faktor-Authentifizierung
- Keine spezielle Hardware nötig, Smartphone/Tablet mit Kamera reicht
- Ist unabhängig vom Browser, keine Installation oder Konfiguration im Browser nötig
- Dieses Verfahren wird auch in anderen Anwendungsfällen (z.B. Online-Banking) verwendet, die gesammelte Erfahrung mit TOTP lohnt sich daher „doppelt“
- Weniger Aufwand für FlexNow-RUB-Support als beim Verfahren mit Chip-Karte
- Akzeptanz bei Anwender*innen:
  - Kommt sehr gut an bei den Studierenden, können z.B. spontan im Bus in die SSS
  - Anscheinend gute Akzeptanz bei Mitarbeiter*innen; wer privates Smartphone/Tablet nicht nutzen will, kann auf das „Hardware-Token“ (siehe Folie 20) ausweichen

Vor- und Nachteile von TOTP

Nachteile von TOTP:

- Man kann sich „aussperren“, wenn man bestimmte Infos nicht mehr hat
- Man braucht ein mobiles Gerät mit Kamera, RUB stellt dafür keine Dienst-Handys
- Bestimmte neue Support-Fälle, siehe folgende Folie „Probleme durch TOTP“
- Ich halte das vorige 2FA-Verfahren (mit Chip-Karte und Lesegerät mit USB-Anschluss) für etwas sicherer, aber schwieriger zu handhaben und praktisch nicht mobil nutzbar

Probleme durch TOTP:
Mitarbeiter*in studiert zugleich an der Hochschule

- Problem 1:
  - Mitarbeiter*in kommt immer in die SSS aber nie ins LM
  - Lösung, je nach Fall:
    - Die Person wird beim Anlegen des Mitarbeiter*innen-Account anders im RBAC behandelt
    - Zusätzlicher Auth-Eintrag im RBAC nötig
    - SQL nötig

- Späteres Problem 2:
  - Mitarbeiter*in ist nun kein*e Student*in mehr
  - Lösung: Die obige Extra-Behandlung wieder rückgängig machen

Doku

Dokumentation

- Wer dieses Dokument als PowerPoint-Datei will, bitte bei peter.fasching@rub.de melden
- Wikipedia zu TOTP: https://de.wikipedia.org/wiki/Time-based_One-time_Password_Algorithmus
- Wikipedia zur 2FA: https://de.wikipedia.org/wiki/Zwei-Faktor-Authentisierung
- Zwei Dokus von uns (FlexNow-RUB-Support): Unter dem Button „Login mit Handy-App“ den Button „Anleitungen & Datenschutz“, auf: https://www.flexnow.ruhr-uni-bochum.de
- Zum „OpenAM-Server“: Im Hochschul-weit erreichbaren Tomcat laufender Dienst, welcher die „ForgeRock Access Management Plattform“ implementiert, der kommerzielle Weiterentwicklung von OpenAM durch ForgeRock: https://www.forgerock.com/platform/access-management
- Zum „OpenAM-Agent“: Komponente („Web Policy Agent“), die in einen Apache/Tomcat installiert wird, wobei im Tomcat das fn2Web läuft: https://backstage.forgerock.com/docs/openam-web-policy-agents/5.9
- Ticket „TOTP als neue Authentifizierungsmethode fürs FlexNow-Web“ der RUB v. 2019: https://tickets.ihb-eg.de/issues/4883