universität innsbruck

Zwei-Faktor Authentifizierung an der Uni Innsbruck

✨ Freie Software 🦬🐧
✨ Offene Standards 🤝
✨ Lokaler Betrieb 🏡

universität innsbruck

Fahrplan

- Projektziele
- Designentscheidungen
- Architektur
- Ablauf
- Lektionen
- Future Work

universität innsbruck

Ziele

- 2FA ist das neue normal (Akzeptanz)
  - Bildungsauftrag
- **Alle** Accounts
- Minimale externe Abhängigkeiten

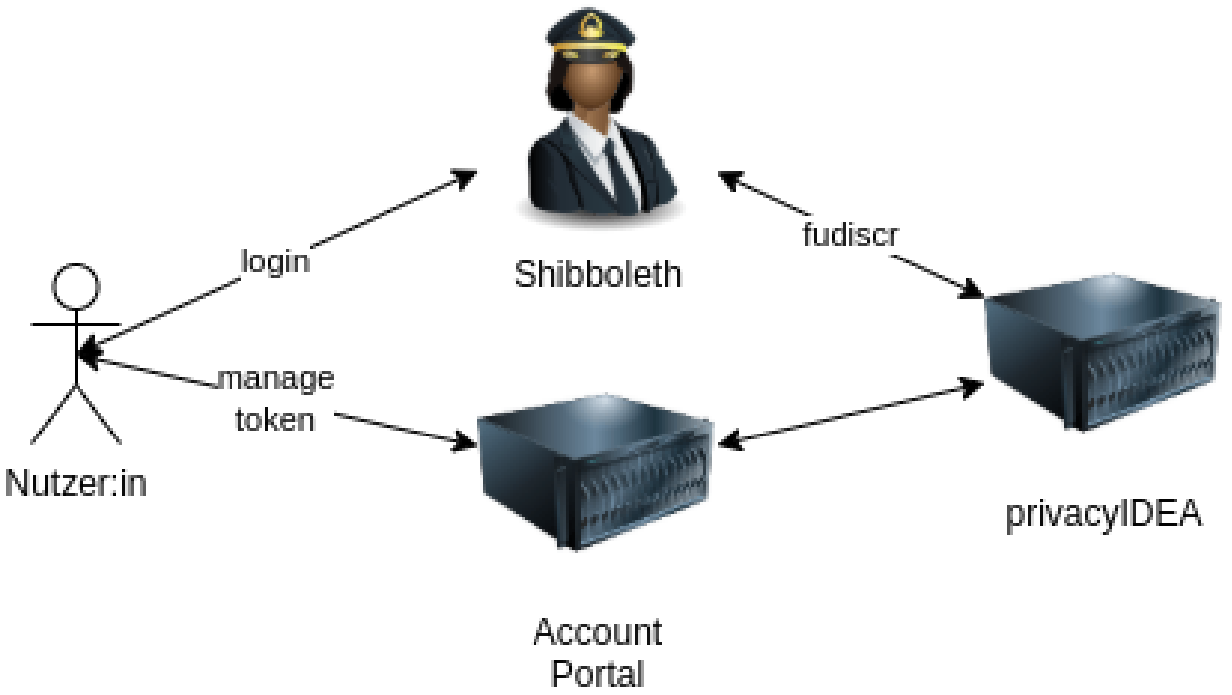
universität innsbruck

Designentscheidungen

- SSO everywhere!
- Offene Standards (TOTP und WebAuthn)
- privacyIDEA

universität innsbruck

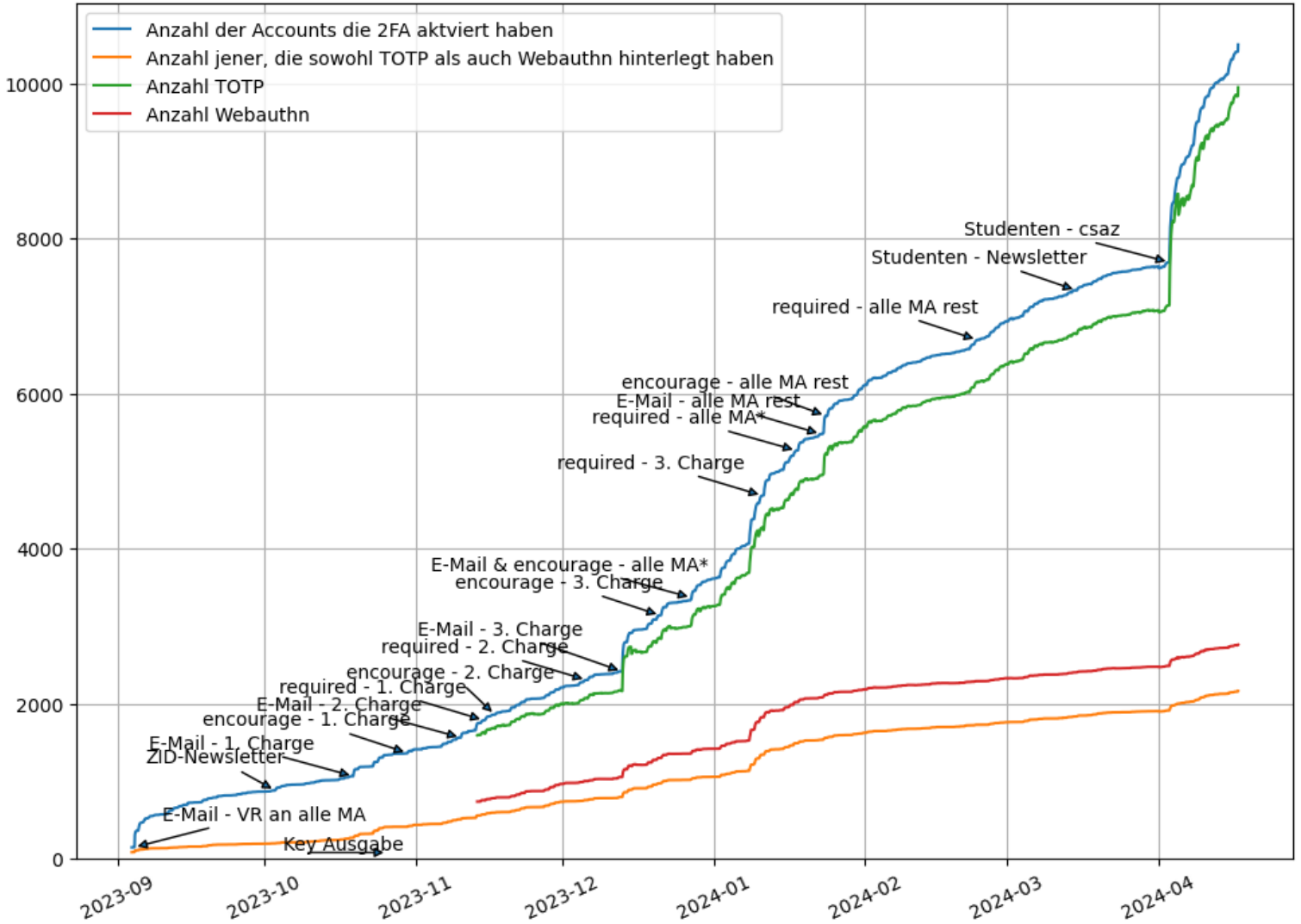
Architektur



universität innsbruck

Ablauf

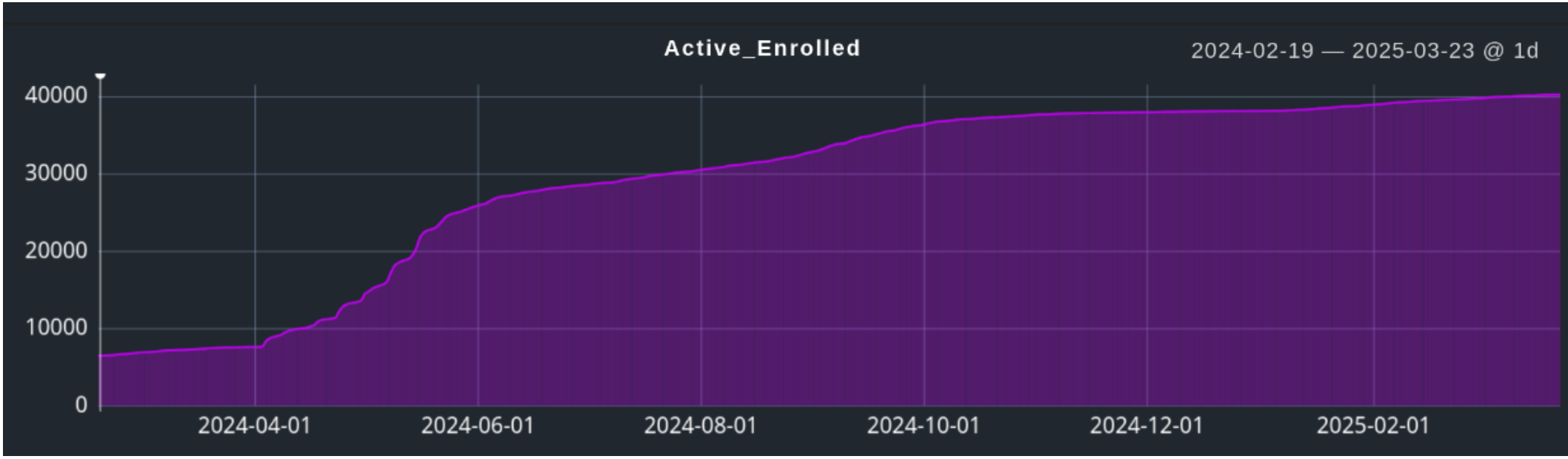
- Planung und Aufbau bis Mitte 2023
- 2023-09 Opt-in Einladung für Mitarbeitende, anschließend Verpflichtung in Chargen
- Ab 2024-03 Rollout Studierende
- Heute: > 40.000 Accounts mit 2FA 🎉



Matthias Weiler

universität innsbruck

Ablauf



universität innsbruck

Lektionen

- UX muss Priorität #1 sein!
  - Registrierungsflow
  - Anleitungen
  - Mailaussendungen
  - Einheitlichkeit (zB keine Unterscheidung nach Netzwerksegmenten)

Öffnen Sie Ihre Authenticator-App

Sie haben noch keine App? Öffnen Sie den Appstore auf Ihrem Mobiltelefon. Suchen Sie nach privacyIDEA Authenticator von NetKnights GmbH und installieren Sie diese App. Weiterführende Informationen dazu finden Sie in der Dokumentation.

Scannen Sie den QR Code mit einer Authenticator-App

Zum Kopieren des Schlüssels klicken Sie hier.

Geben Sie das generierte Einmalpasswort für Token *TOTP472354F9* ein

Verifizieren

Abbrechen

universität innsbruck

Lektionen

- Durchgängiges SSO ist das halbe Projekt
  - Sicherheit ist nicht das Gegenteil von Usability!
    - nur ein Login pro Tag – einheitliche Session-Lifetime
  - Etablierter Standard (SAML, OIDC)
  - Sicherheitsgewinn
    - Die Zugangsdaten dürfen ausnahmslos auf “idp.uibk.ac.at” eingegeben werden
    - lockout, rate-limiting, logging an einer Stelle

universität innsbruck

Lektionen

- FIDO2/WebAuthn ist gekommen um zu bleiben
  - Fokus auf TOTP war 2023 die richtige Wahl
  - Security Keys und Windows Hello PIN für Mitarbeitende
  - Gute Erfahrungen mit Yubico Security Key (nicht YubiKey)
  - Studierenden Securtiy Keys zum Kauf anbieten macht Sinn #a11y

universität innsbruck

Lektionen

- Softwareempfehlungen sind schwierig
  - nicht in unserem Einflussbereich
  - privacyIDEA Authenticator (App)
  - KeePassXC “zu schwierig”
  - Cloud-Sync oder lieber kein Backup?

universität innsbruck

Lektionen

- Supportaufwand
  - Leute verlieren “something they have” öfter, als sie ihr Passwort vergessen
  - Reset-Prozess optimieren (Ausweiskopie? Staatlicher IDP? Videoident? Backup-Mailadresse?)
  - “Bitte zweiten Token als Backup einrichten”

universität innsbruck

Lektionen

- privacyIDEA
  - einzelne VM mit lokaler DB. (daily peak: 3k Anmeldungen pro Stunde) Cold-standby für Wartungen
  - wir hatten Probleme mit unserer Oracle DB – Umstieg auf MariaDB

universität innsbruck

Future Work

- E-Mail
  - Clients können OAuth 2.0 für IMAP/SMTP nur mit wenigen Anbietern (Thunderbird Issue)

universität innsbruck

Future Work

- WLAN
  - https://www.geteduroam.app/about/goals/
  - “we develop server software that can issue client certificates to be used with EAP-TLS”

universität innsbruck

Future Work

- SSH
  - low-hanging fruit: ed25519-sk / ecdsa-sk Schlüssel mit Security Key (und PIN)
  - echtes SSO mit OIDC?

universität innsbruck

Future Work

universität innsbruck

Dankeschön! <3

- Matthias Weiler, BSc
- Informationssicherheitsbeauftragter
- E-Mail: matthias.weiler@uibk.ac.at
- Matrix-ID: @matthias.weiler:uibk.ac.at
- Fediverse: @MatthiasWeiler@social.uibk.ac.at

Foto: Agnieszka Kulowska