Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

Technische und organisatorische Integration einer Multi-Faktor-Authentifizierung

am Beispiel eines Hochschulrechenzentrums

04.02.2022 | Miran Mizani, David Schmitz, Jule A. Ziegler, Stefan Metzger, Helmut Reiser | Leibniz-Rechenzentrum

Passwortschutz ist allein kaum mehr ausreichend

Anwender:innen wählen schwache Passwörter. → **Risiko der Account-Kompromittierung** ← automatisierte und teils gezielte Angriffe

- *Privilegierte Accounts*
- *Studi-Kennung ist mehr als „nur WLAN“*

Passwort-Security am Leibniz-Rechenzentrum

- Passwort-Qualitätsvorgaben
- live-Pwned-Check bei PW-Änderung
- dynamische Reaktion auf PW-Leaks
- wöchentlicher Check auf Kompromittierung

Mehr-Faktor-Authentifizierung

Das LRZ etablierte 2FA zuerst für die typischsten Anwendungsfälle

Use Cases

UC1: Fernwartung per **SSH und RDP**

UC2: Telearbeit per **VPN**

UC3: Desktoplogin (**Windows, Linux, Mac**)

UC4: Login an **Webapplikationen**

UC5: Ausgabe, Verlust, temp. (Gast)zugänge **Tokenmgmt & Self-Service**

Anforderungsanalyse

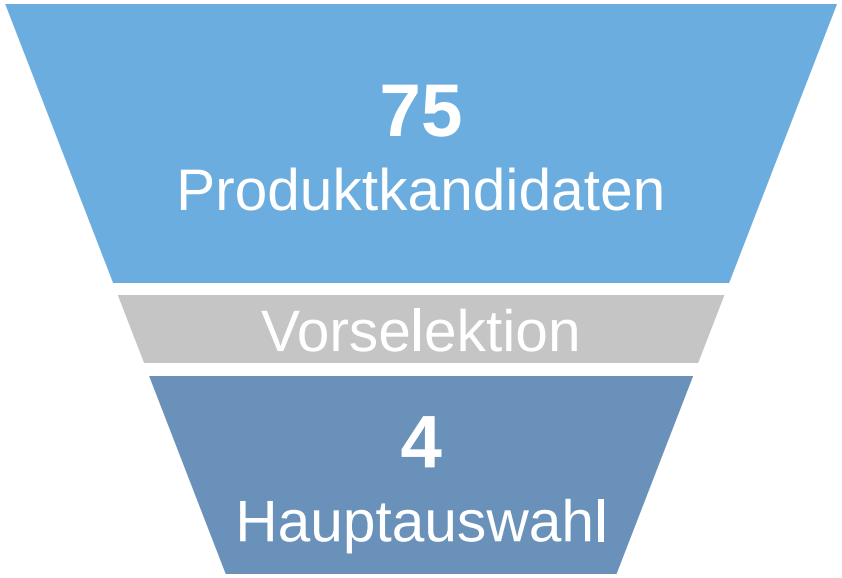
109 Einzelanforderungen
in 30 (Unter-)Gruppen

Anforderung	Gewichtung
1 Rahmenanforderungen *Rahmenbedingungen für das gesamte 2FA-System des LRZs*	2
2 Einrichtungsaufwand *Zeit- und Ressourcenaufwand der Implementierung und Einführung der 2FA-Lösung*	3
3 Verwaltung, Wartung, Erweiterbarkeit *Administrative Tätigkeiten wie bspw. Hinzufügen neuer Nutzer oder Vergabe von temporären Zugängen (Szenario 5)*	4
4 Sicherheitsniveau *Anforderungen aus Perspektive der IT-Sicherheit*	3
5 Kosten(-effizienz) *Finanzielle Aspekte für das LRZ sowie einzelne Anwender*	2
6 Bedienkomfort *Der Authentifizierungsvorgang aus Anwendersicht*	3
7 Anwendungsbereiche *Anforderungen aus den Einsatzszenarien 1 bis 4*	4

1=wünschenswert, 2=relevant, 3=wichtig, 4=sehr wichtig bzw. essentiell

Anforderungskatalog und Produktbewertung:
https://www.nm.ifi.lmu.de/pub/Fopras/miza18/

Marktanalyse und Produktauswahl



privacyIDEA AUTHENTICATION SYSTEM

www.privacyidea.org

Bulk-Import und Auto-Rollout von Hardwaretoken

Tokentypen und Zahl nicht beschränkt

Attraktives Preismodell

open-source

Organisatorische Integration

Wahl der Zweitfaktoren

Tokentypen am LRZ

YubiKeys

- Hardwaretoken: U2F, (T)OTP, …
- 45€ pro Token
- YK als Tastatur

Standardtoken für LRZ-Beschäftigte

Soft-Token

- Smartphone-App: TOTP
- kostenfrei
- OTP abtippen

für große Nutzerzahlen und als Backup bei Verlust

PUSH-Token

- Push-Benachrichtigung
- kostenfrei
- „Ja“/„Nein“ klicken

wo Anpassungen der GUI nicht möglich

Token-Management und Self-Service

Ziel:
Schlanke Abläufe und möglichst wenig Supportaufwand für die Identity-Gruppe

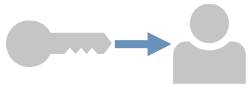
→ Automatisierung, Self-Service + umfangreiche Doku!

Self-Service-Portal

- Ausrollen (weiterer) Token (z.B. Soft-Token: TOTP, PUSH)
- Sperren von Token bei Verlust

temp. Token & -Verlust

- Max. Token-Gültigkeitsdauer für z.B. Gäste oder Tages-Ersatz
- Anwender:in kann bei Verlust ihren Backup-Token nutzen



Credential binding

1. YubiKey-Ausgabe über Benutzersekretariat mit Identitätsfeststellung + Hinweisblatt
2. Aktivierung über Self-Service-Portal

KAUM First-Level-Support durch Identity-Gruppe war erforderlich

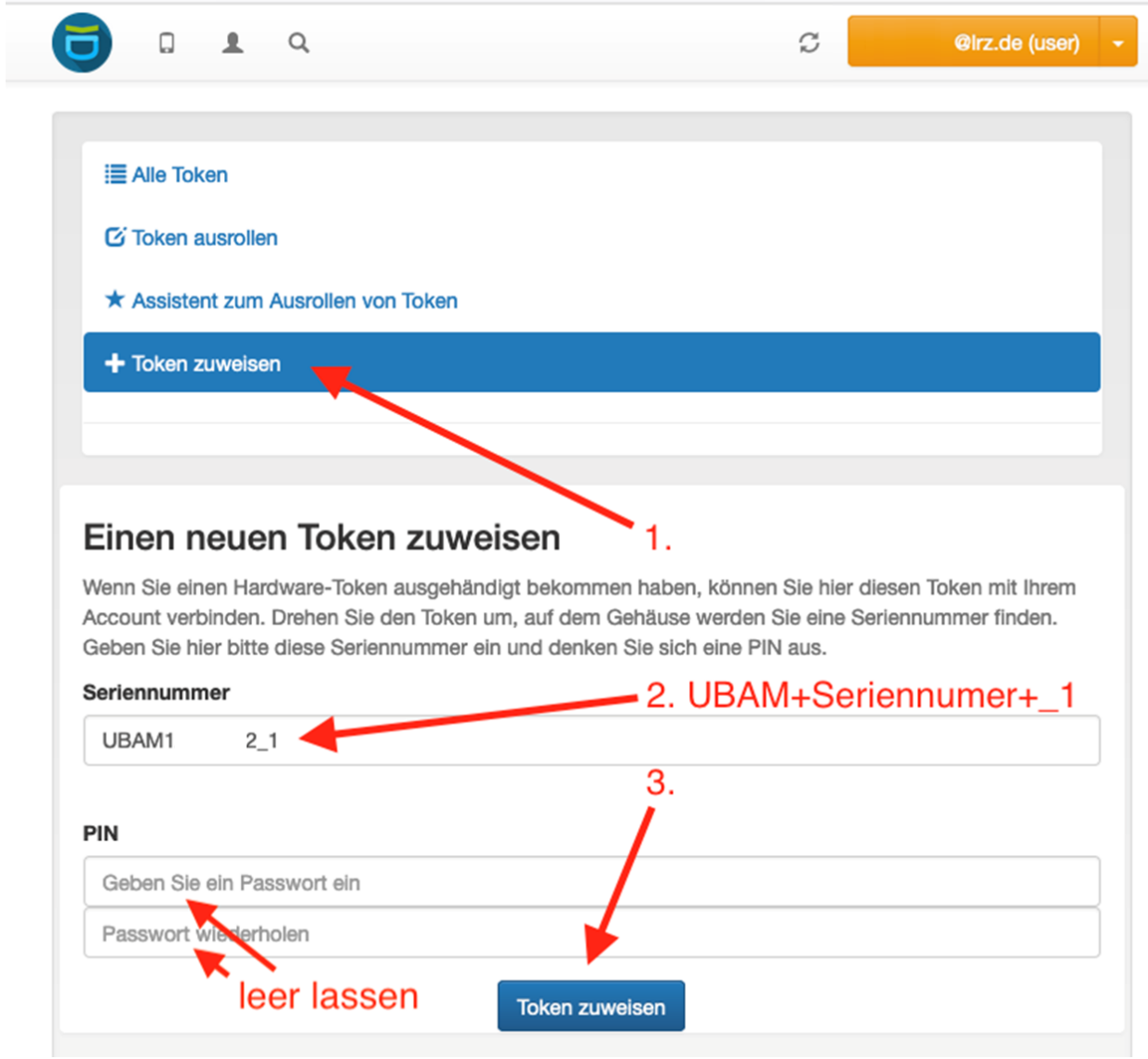
Hardware-Tokenrollout as easy as…

„Nimm dir einen Token vom Stapel“

Willkommensseite beim Erstlogin im Self-Service-Portal

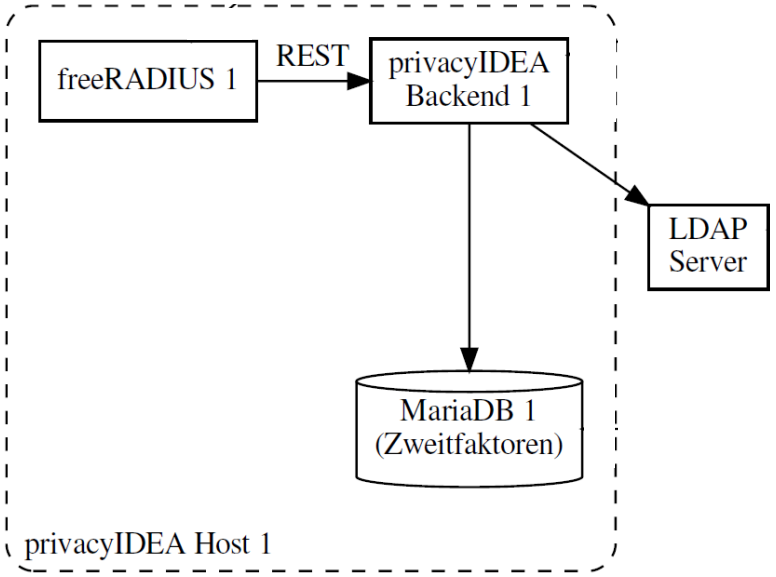
1. „Token zuweisen“
2. Seriennummer des YubiKeys abtippen
3. Fertig

> *Vorbereitend:*
> Bulk-Programmierung der YubiKeys und Seed-Import mittels *PI-Admin-Tool*
> https://github.com/privacyidea/privacyideaadm

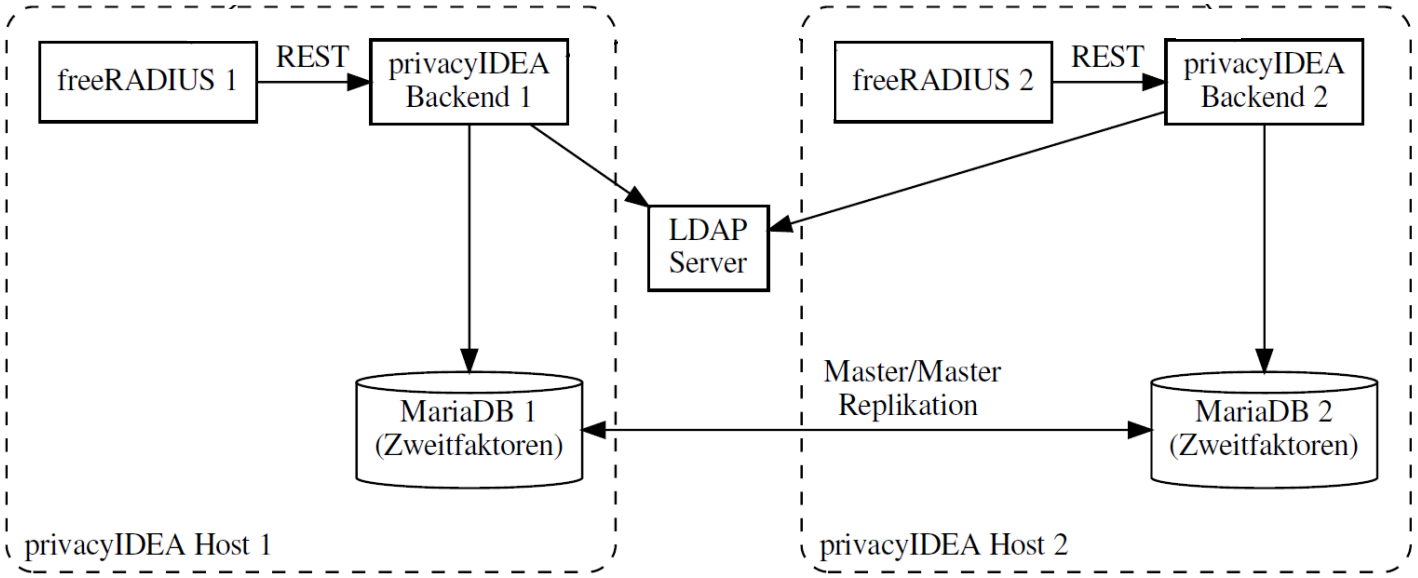


Technisches Setup

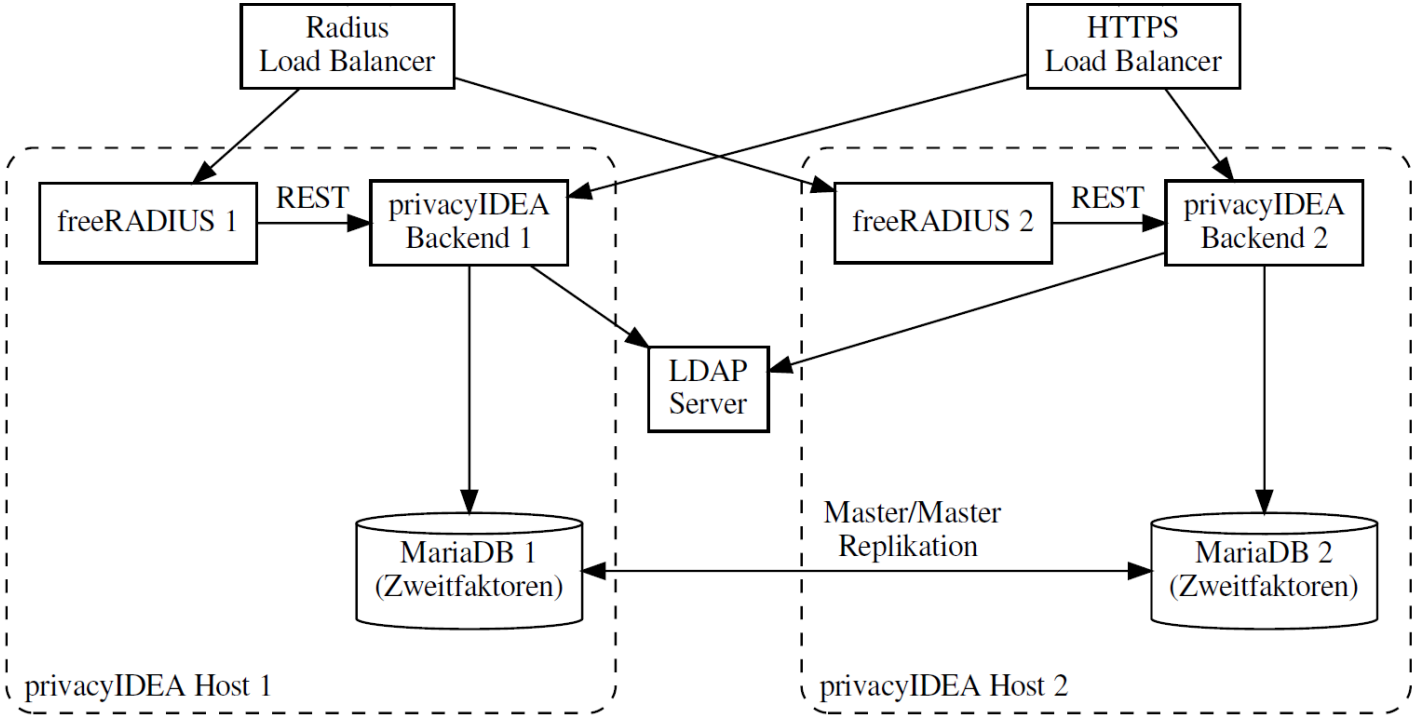
privacyIDEA-Backend



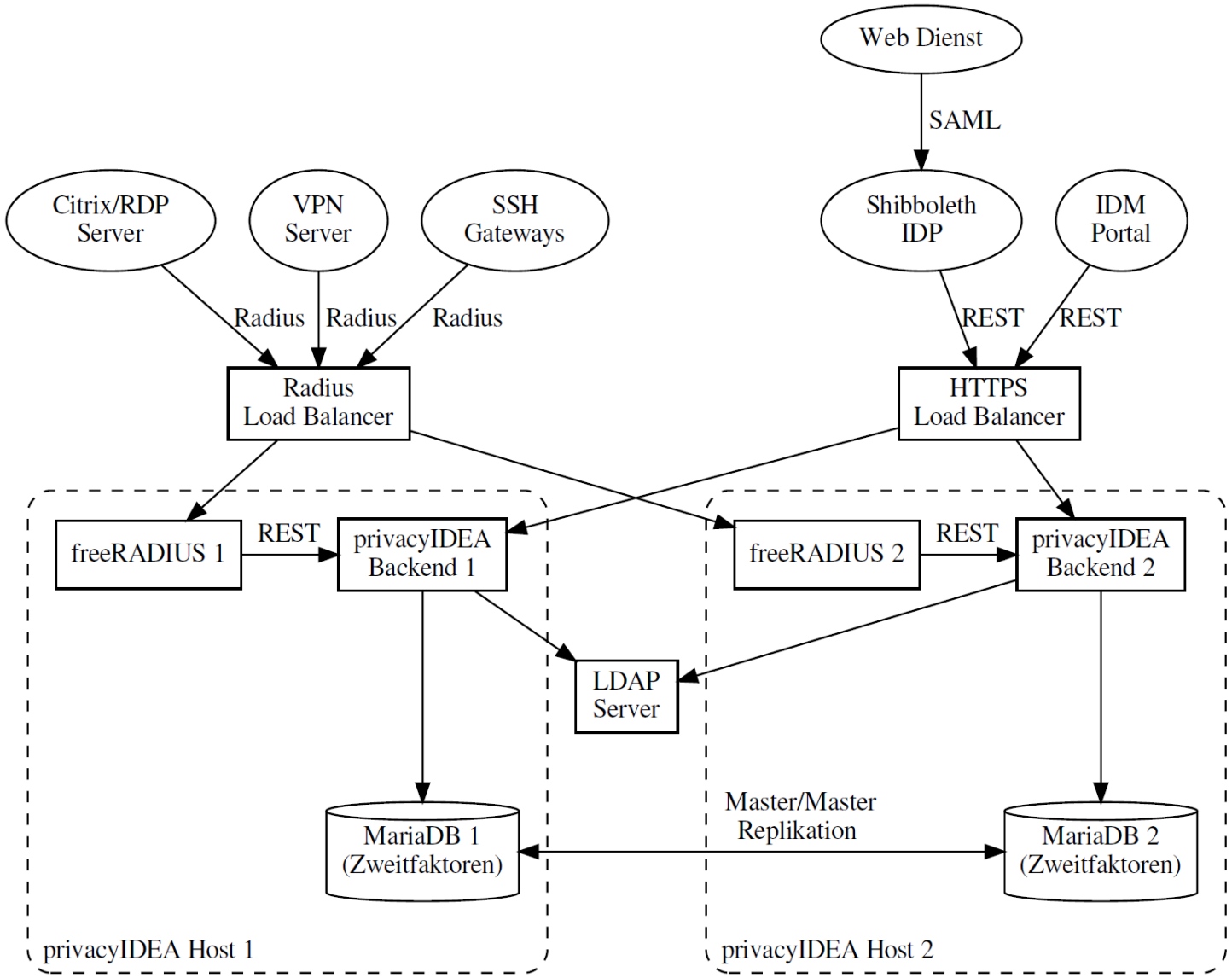
Redundanz


freeRADIUS 1
REST
privacyIDEA Backend 1
freeRADIUS 2
REST
privacyIDEA Backend 2
LDAP Server
Master/Master Replikation
MariaDB 1 (Zweitfaktoren)
MariaDB 2 (Zweitfaktoren)
privacyIDEA Host 1
privacyIDEA Host 2

Load-Balancing (RADIUS und HTTPS)



Anwendungen



UC1: SSH- und RDP-Gateways

SSH

an SSH-Gateways
OTP | PUSH
via RADIUS

alternativ via pam-python-Skript und REST-API – jedoch nur Python2

RDP

am Citrix Terminalserver
OTP | PUSH
via RADIUS

---

am RDP-Gateway
PUSH
via RADIUS

Aber: Kein Eingabefeld für OTP auf Login-Screen möglich
→ PUSH-Token

(erfordert weltweite Erreichbarkeit des privacyIDEA-Servers)

UC2: VPN & UC4: Webapplikationen

VPN

mit Cisco AnyConnect
OTP | PUSH
via RADIUS

mit eduVPN
OTP
via Shibboleth

Webapplikationen

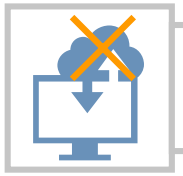
an Webdiensten
OTP
via Shibboleth

an Eigenentwicklungen
OTP | PUSH
via REST-API

UC3: Desktoplogin

Deadlock-Gefahr!
wenn (noch) keine Internetverbindung

→ 2F-Validierung muss auch offline verfügbar sein!



Offline-Token → HOTP (out-of-sync…?)

- **Linux:** nur via pam-python *(Python 2)*
- **Windows:** HOTP erfordert Windows Credential Provider
  -> Probleme bei Windows-Updates
- **Mac:** ebenfalls nur HOTP

→ Vorerst kein 2FA für lokalen Desktop-Login am LRZ

Lessons Learned

Organisatorisch

Veränderung gewohnter Arbeitsweisen

→ Mehrstufige Einführung der 2FA (Scope)

+ Pilotbetrieb

+ Übergangszeit (mit 2FA optional)

Wahl der Tokentypen

- Wunsch nach *Smartphone-App → Hardwaretoken*
- Softtoken parallel als Backup-Faktor und für große Nutzerzahlen

Technisch

2FA für den 2FA-Server

SSH mit 2FA – Wartung im Fehlerfall?

→ *lokale 2FA via TOTP-pam-Modul*

2FA

2FA für Self-Service

Token-Rolloutfunktion schützen

→ *+ Backup-Tokens*

parallele 1FA und 2FA

Oftmals erforderlich/ratsam!

→ *abhängig von Nutzerrolle, Gruppe,…*

1FA || 2FA

Fazit und Ausblick

Zugänge sind sicherer

im Alltag kein spürbarer Mehraufwand für 2FA

kaum First-Level-Support
Bulk-Rollout, Doku & Self-Service

Roadmap

2FA für weitere (Web-)**Dienste** des LRZ
Code-Snippets für Entwickler/Admins

2FA für weitere **Nutzerkreise**
Schnelle Integration mit Shibboleth

LRZ im Projekt *Bayern2MFA*

Beratung und KnowHow
zur Unterstützung der 2FA-Einführung

Technische und organisatorische Integration einer Multi-Faktor-Authentifizierung

am Beispiel eines Hochschulrechenzentrums

04.02.2022 | {Miran.Mizani, David.Schmitz, Jule.Ziegler, Stefan.Metzger, Helmut.Reiser}@lrz.de