
# Sicher in die digitale Zukunft: Strategischer Rollout von Multi-Faktor-Authentisierung mit eduMFA und Shibboleth

Harald Strack und Lucas Gehrlein | Berlin | 17.03.2026

# Der Schlüssel zum reibungslosen MFA-Rollout an Hochschulen

## Dynamische Nutzerführung im Rolloutflow

Das System unterscheidet automatisch zwischen sanfter Erinnerung (Warning) und verpflichtender Einrichtung (Enforcement).

## Automatisierung statt manueller Prozesse

Event-basierte E-Mail-Token oder TOFU-Szenarien (Trust On First Use) erlauben flexiblen Rollout und Betrieb.

## Entlastung durch Self-Service-Flows

Nutzer verwalten ihre Primär-, Fallback- und Recovery Token eigenständig in einem geführten Prozess im Loginfluß.

## Präzise Steuerung durch Predicates

Flexible Regelwerke entscheiden exakt, welche Nutzergruppen wann welche Faktoren registrieren müssen, um den Betrieb nicht zu stören.

# Agenda

1. Motivation
2. Grundlagen MFA und Token Mix
3. Integration in Dienste und Infrastruktur
4. MFA Rolloutverfahren
5. Details zum RolloutFlow Plugin
6. Ausblick

# Treiber und Auslöser

Motivation für die Entwicklung des MFA-Rollout Plugins

## Sicherheitsdruck

Zunehmende Ransomware durch besseres Phishing mit KI

Verschärfte Vorgaben durch BSI & Ministerien

**Tipping Point: MFA Rollout am IDP**

**Initiative der FU Berlin**

**+**

**Erfahrung in der OSS Entwicklung bei ssystems**

## Standardlösung

UI/UX sehr aufwendig, vielen war die Tragweite des Rollouts und Betriebs nicht klar.

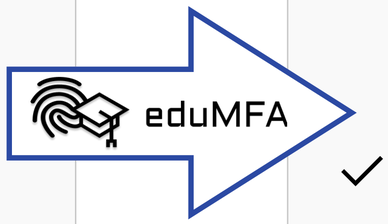
OIDC für Cloud-Dienste, SSO, Verbesserung Usability und Self-Services

# Projektziele

Digitale Souveränität, Vermeidung von Vendor-Lock-In

## Risiken & Defizite

- ⚠ MFA installiert aber nicht in der Breite ausgerollt
- ⚠ Ungeschütze Zugriffe auf kritische Hochschulanwendungen
- ⚠ Fehleranfällige, manuelle oder dedizierte Verwaltungsprozesse




## Zielsetzung

- ✓ Erfüllung der “Vereinbarung zur Cybersicherheit” (NRW/BSI-Mandate bis 2026)
- ✓ Flächendeckende Absicherung der Authentifizierungs-Intrastruktur
- ✓ Automatisierte, systemgestützte Rollout-Prozesse für hohe Nutzerzahlen direkt am IDP

# NIST AAL und BSI Anforderungen

Der NIST-Standard 800-63-4 definiert drei Authenticator Assurance Level (AAL)

## NIST AAL1

- Einzelfaktor (Passwort)
- Sessiondauer: bis zu 30 Tage

### BSI Basis-Anforderung:

MFA-Einsatz muss geprüft werden.

## NIST AAL2

- Zwei Faktoren mit Kryptografie (z.B. TOTP).
- Typisch Studierende
- Sessiondauer: 12 Stunden (30 Min Inaktivität)

### BSI Standard-Anforderung:

Accounts mit weitreichenden Berechtigungen SOLLTEN mit MFA geschützt werden. NRW: faktisch ein MUSS.

## NIST AAL3

- Zwei Faktoren, davon einer Hardware-basiert (z.B. FIDO2).
- Typisch Nicht-Studierende
- Sessiondauer: 12 Stunden (15 Min Inaktivität)

### BSI Erhöhter Schutzbedarf:

Sichere MFA via Token/Chipkarte zwingend.

# Human-Centered Security (HCS) I

Sicherheit und Usability dürfen keine Gegensätze sein, mangelnde Nutzerfreundlichkeit schwächt Sicherheit

## Aufwandsminimierung für den Nutzer

Sicherheitsmaßnahmen und -hinweise **nutzerfreundlich** gestalten, sodass sie möglichst wenig Zeit und kognitive Ressourcen beanspruchen

## Realistische Risikoeinschätzung

Vorgaben sollten sich nicht nur am absoluten "Worst-Case" orientieren, sondern ein **durchschnittliches Risiko** abbilden.

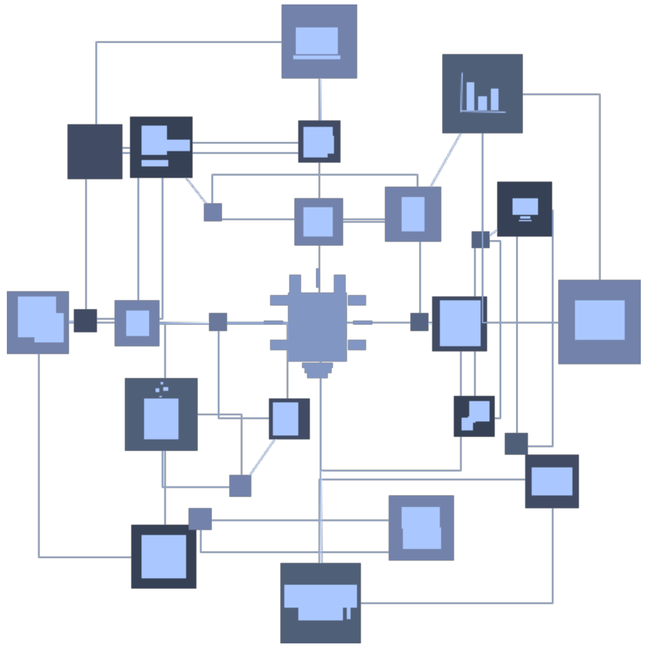
- Geht es um mehr als Abwehr von Phishing?
- TOTP für Studierende?

## Fokussierung und Aktualität

Sicherheitsmaßnahmen **priorisiert** und **gruppenbezogen**. Veraltete Hinweise sollten regelmäßig zurückgezogen oder überarbeitet werden. Szenarien Mitdenken: **E-Assessment**...

## Session Dauer und Risikobasierte Authentifizierung (RBA)

Sessiondauer **kontextbezogen** gestalten. Kontext auswerten (IP, Uhrzeit, ...) und MFA am Risiko ausrichten



# UDS Framework

Welcher 2. Faktor ist der richtige?

| | Usability | Deployability | Security | |
|---|---|---|---|---|
| TOTP-App (Smartphone) |  |  |  | Etablierter Standard, hohe Akzeptanz, anfällig für Phishing, gut skalierbar. |
| FIDO2-Key (Hardware) |  |  |  | Sehr sicher, physisches Verlustrisiko, teuer |
| Passkeys (Software) |  |  |  | Guter Standard mit Sync- und Kompatibilitätshürden. |
| App-Passwörter |  |  |  | Übergangslösung für Legacy-Systeme, schlechte UX. |

Jesske, Philipp (2026). Einführung sicherer Authentifizierung an Hochschulen, Diplomarbeit, TU Dresden

# Unvollständige MFA-Abdeckung

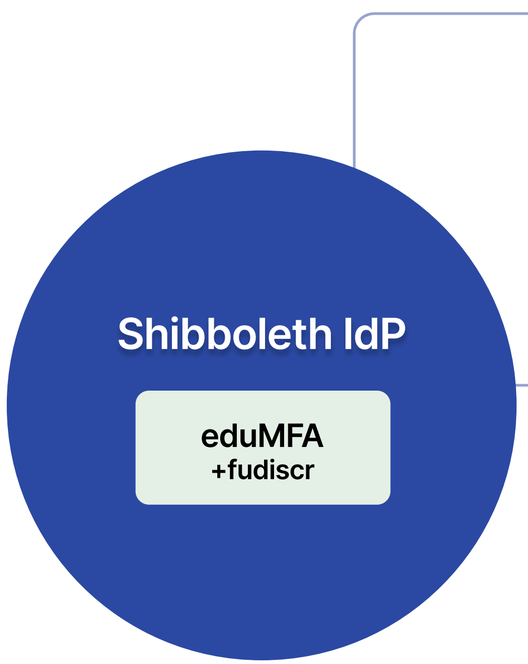
Heterogene IT-Landschaften

### Microsoft / Cloud

- MS365 oder Google-Workspace
- On-Premise: Username/ Passwort

### VPN und eduroam®

- CAT für eduroam®
- CISCO ISE™
- FortiAuthenticator™
- ....




### WWW Services

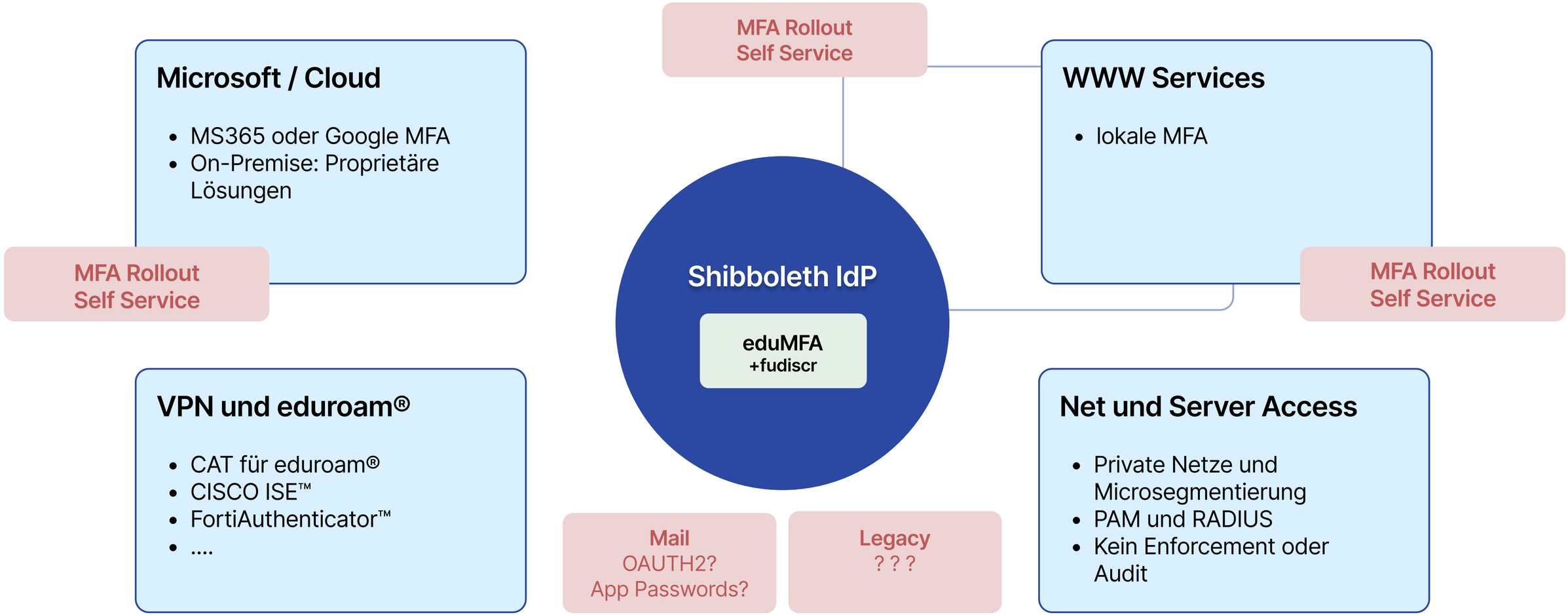
- lokale MFA

### Net und Server Access

- Private Netze und Microsegmentierung
- 802.1x

# Autarke MFA-Lösungen

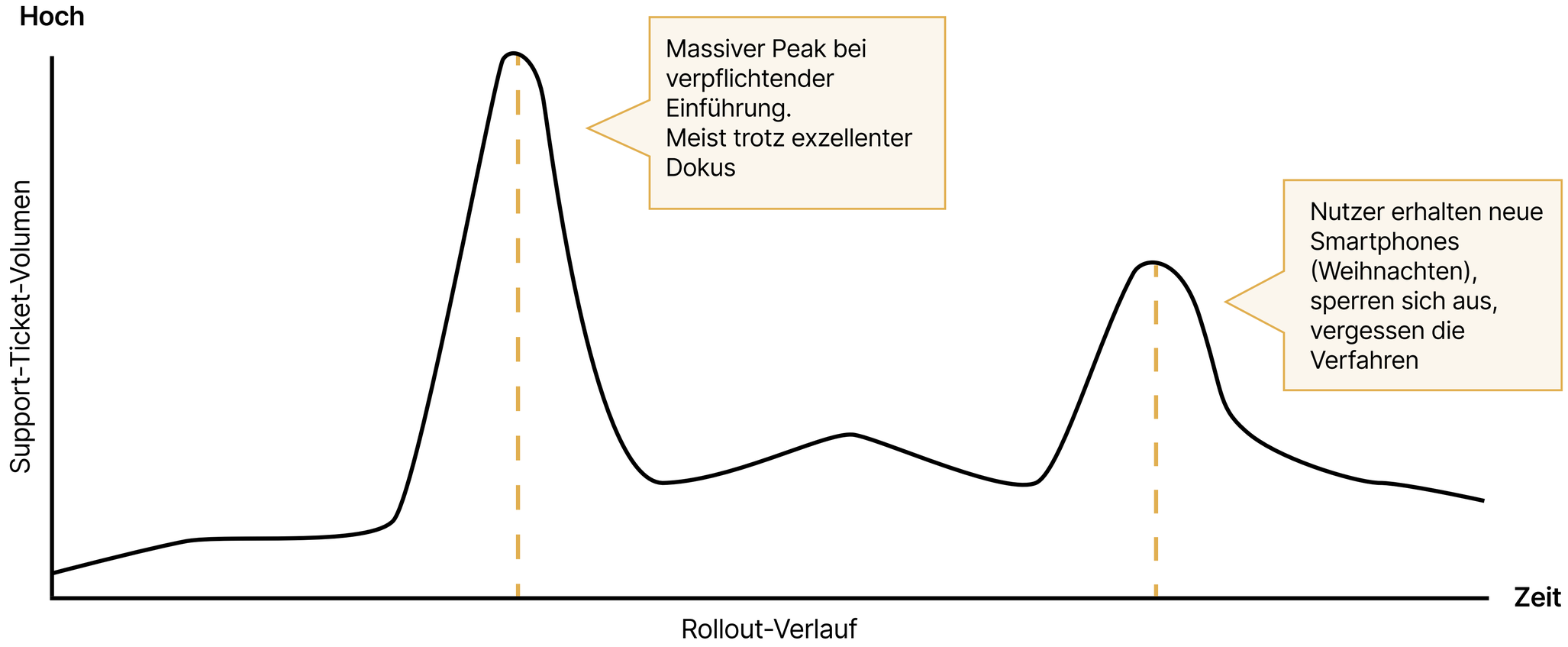
Uneinheitliche MFA, sehr schlechte UX und eingeschränkter Token Mix



# Human-Centered Security (HCS) II

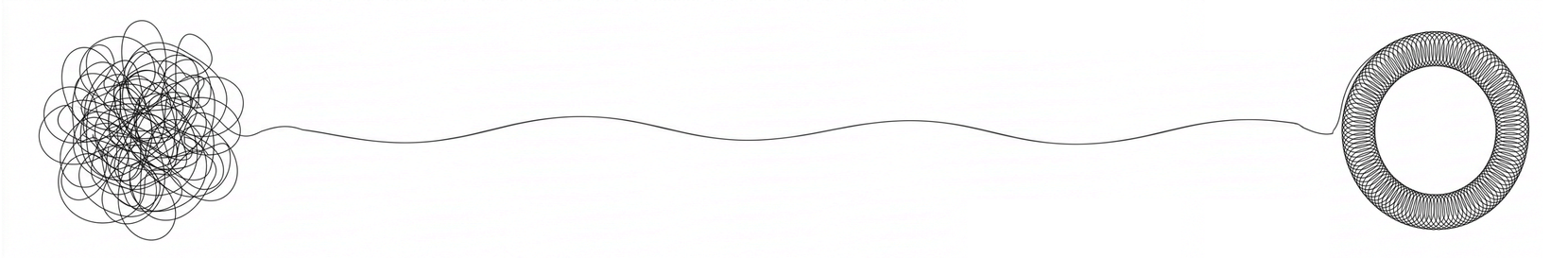
Support als Flaschenhals

Supportaufwand misst Usability: Schlechte Usability führt zu vielen Tickets. Bei komplexen Rollouts, wie einer MFA-Umstellung, können an einer Hochschule mit 40.000 Personen **über 500 Tickets pro Tag** entstehen.



# Entscheidende Vorteile für Nutzer und Betrieb

Anstatt die Nutzer auf ein separates Portal zu schicken, „passiert“ die Einrichtung einfach während eines regulären Logins



| Ohne Plugin | | Mit Rollout Plugin |
|---|---|---|
| Ressourcenintensive langwierige Konzeption und Entwicklung von Portalen notwendig | **Entwicklungshürden** | Konfiguration und Integration |
| eduMFA UI erfordert technisches Verständnis vom Nutzer | **Technische Vereinfachung** | Token-Registrierung tief im IdP integriert |
| Ablauf unterbrochen, Umleitung auf separates Portal und kein Drive-by Rollout | **Nutzererfahrung** | Rollout im Anmeldefluss in vertrauter UI/UX, nicht aus Arbeitsablauf gerissen, verständlich |
| Suboptimale UX führt zu Support-Chaos | **Support** | Verbesserte Benutzerführung und Filter entlasten Helpdesk |

# Rollout "sanft" und nutzerfreundlich gestalten

Nutzer nicht abrupt durch den Zwang zu einem zweiten Faktor überrumpeln, sondern schrittweise an die neue Technik heranführen

## Phase 1: Advisory MFA (empfohlene Phase)

### Reminder Flow

Nutzer ohne Token erhalten nach dem Passwort-Login einen Hinweis auf der IdP-Seite

**Regel:** Keine E-Mail-Kommunikation mit Links (Vermeidung von Phishing-Konditionierung). Optionale Nutzung fördert Akzeptanz.

## Phase 2: Mandatory MFA (verpflichtende Phase)

### Rollout Flow

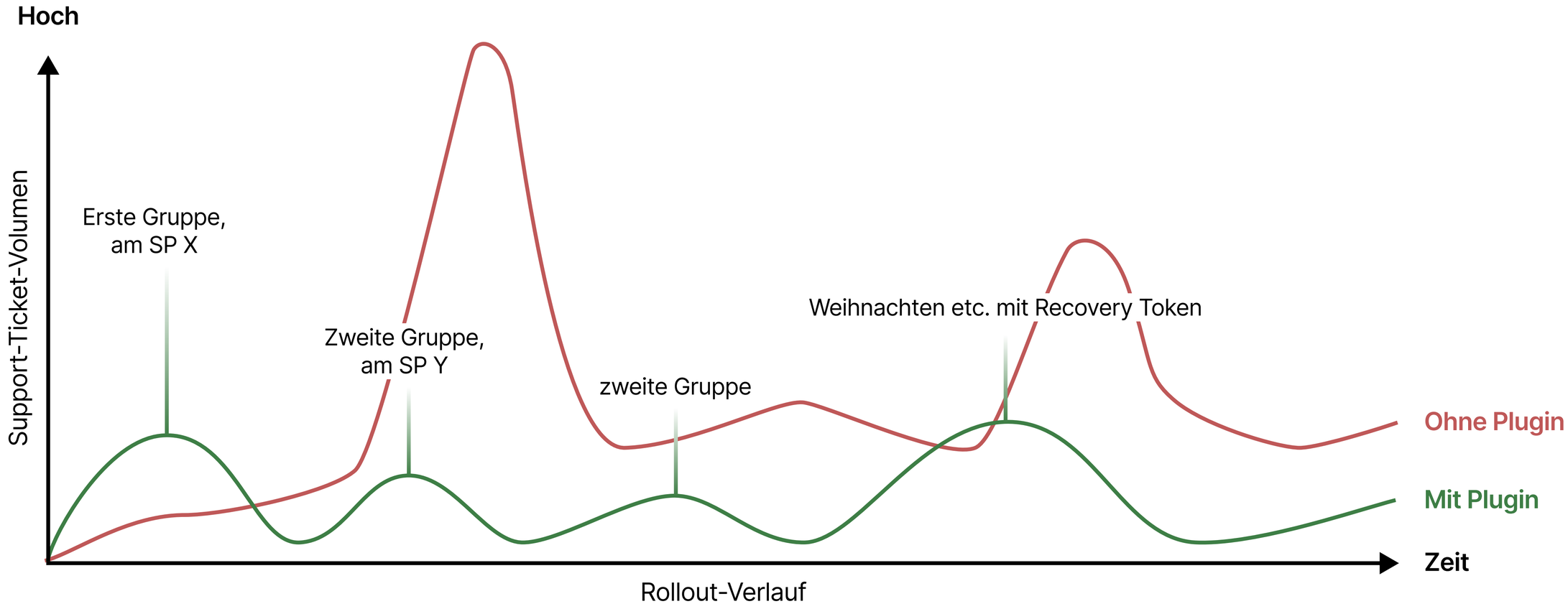
Registrierung wird im Authentifizierungsprozess erzwungen (via Shibboleth Plugin)

**Filter-Kriterien:** Stufenweise Aktivierung nach Dienst, LDAP-Personengruppe (Fakultäten?) oder IP-Bereich (Intern vs. Extern).

# Human-Centered Security (HCS) III

Supportaufkommen steuern

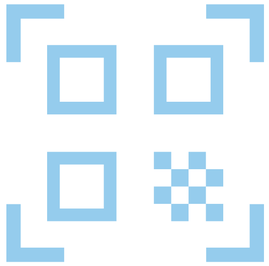
Supportaufwand misst Usability: Gute Usability führt zu weniger Tickets. Bei schrittweisen Rollouts kann an einer Hochschule mit 40.000 Personen das **Ticketaufkommen gesteuert** werden. Recovery Token unterstützen den Betrieb.



# Recovery- und Registrierungstoken

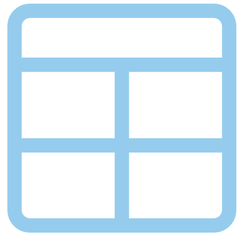
Verlust bzw. Ersatz von Geräten kommt häufiger vor als das Vergessen von Passwörtern

## TOTP (Time-based One-Time Password)



Vollständig kompatibel mit gängigen Authenticator Apps. Können auch per Brief als Registrierungstoken ausgerollt werden.

## Indexed Secret (Token Matrix) / TAN-Listen



Das Plugin installiert Standard-PDF Templates: anpasspar mit eigenen Zeichen C0 bis C80. Alternativ TAN-Listen, die sich verbrauchen.

## Einmalcodes (OTP)

Klassische Einmalcodes per SMS oder E-Mail mit bekannten Einschränkungen.

# Rollout mit TOFU und Vergabe von Recovery-Token

Nur sinnvoll mit entsprechendem Self-Service-Portal

**MFA einrichten** →  → 

Der Fokus: immer möglich, sofort deploybar und kein Registrierungstoken not-wendig.

Der Nutzer muss ein Codematrix speichern. Auf dem Smartphone ggf. lästig.

Ggf. auch mehrere Token erlauben.

https://oc.ssystems.de/paella7/ui/watch.html?id=139c4c2d-c5ef-43ca-984c-16994be01586

# Rollout mit Registertoken

E-Mail / SMS Challenge oder PUK ähnliches Verfahren, Snail Mail

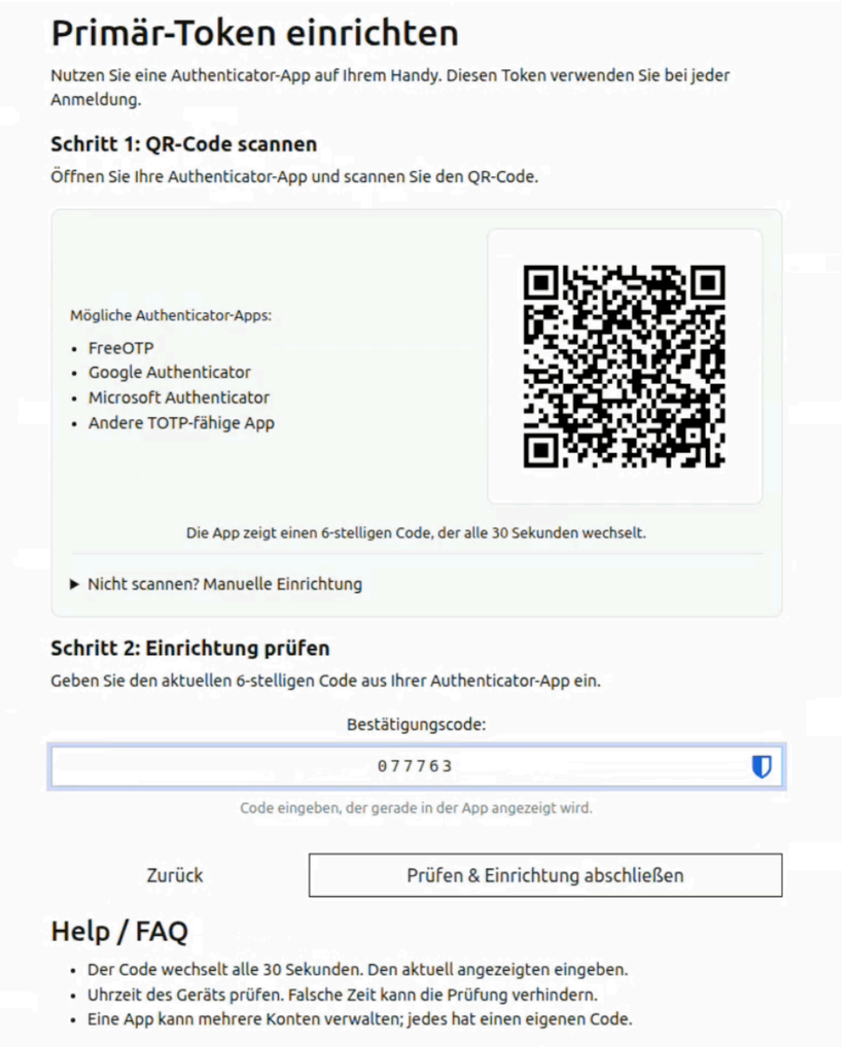

Der Fokus: Keine Recovery-Token-Vergabe, bester Anmeldefluss.

Die Challenge wird verifiziert, Token Mix kann registriert werden. Am Smartphone angenehmer. Kann auch als Recovery-Flow eingesetzt werden.

https://oc.ssystems.de/paella7/ui/watch.html?id=4b2acfde-f722-496c-ae0d-e3b3894aae7d

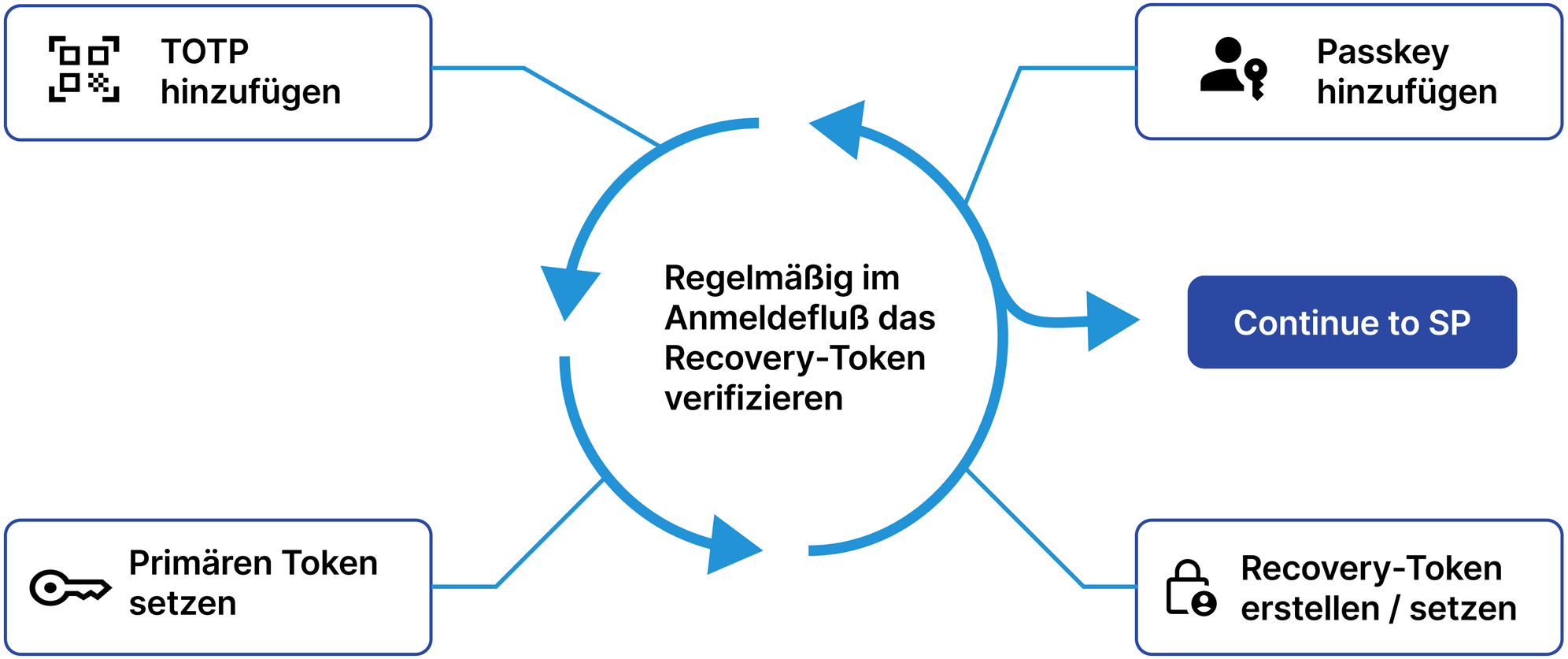
# Rollout mit Registertoken - Beispiel

UI/UX ist individuell anpassbar



# MFA Self-Service am IDP

Recovery-Token ist Voraussetzung für Self-Service




https://oc.ssystems.de/paella7/ui/watch.html?id=c111aeb8-78c6-4e60-98df-f47dc05cb0c9

# MFA Recovery-Token

Beispiel: Recovery-Token-Matrix für Wiederherstellung nutzen

## Zwei-Faktor-Authentifizierung

Bitte nutzen Sie Ihre Recovery-Token-Matrix, die Sie bei der MFA-Einrichtung heruntergeladen haben, und tragen Sie die folgenden Positionen daraus ein:

**G2** **H1**

Geben Sie die Zeichen dieser Positionen der Reihe nach ein, ohne Leerzeichen.

Alternativ können Sie auch die folgenden Token verwenden:

totp - TOTP00094ACB - edumfa_testuser@mfarollout

Prüfen

Token-Challenge neu starten

MFA Self Service | English version

Impressum | Help / FAQ | Dunkles Design

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| A | 6 | b | E | G | d | j | H | r | t |
| B | P | J | H | s | q | h | h | h | M |
| C | W | h | 3 | L | f | q | v | U | 7 |
| D | f | p | 8 | 9 | Q | 4 | T | W | d |
| E | 3 | T | B | j | C | S | D | S | b |
| F | m | j | p | h | b | V | E | 5 | g |
| G | h | a | U | 6 | a | C | Q | 5 | h |
| H | 2 | b | 5 | 3 | p | 8 | s | 7 | Q |
| I | G | U | t | G | o | U | 8 | t | C |

# Verantwortliches Betriebskonzept

MFA- und IdP-Systeme sind ein "Single Point of Failure"

## Hochverfügbare Systemarchitektur

- ✓ Active/Passive oder Active/Active
- ✓ Datenbankreplikation

## Backup

- ✓ Umfassendes Datenbank- und Policy-Backup
- ✓ System-Backups

## Zero Downtime Upgrades

- ✓ Staging-Systeme und Rollentausch im Cluster
- ✓ Versionierung (Infrastructure as Code)

## Monitoring

- ✓ Zentrale Überwachung (Login-Szenarien schwierig)
- ✓ Incident- und Response-Management

## Systemsicherheit

- ✓ Systemhärtung und Updates
- ✓ Reglementierter administrativer Zugriff

## Hochschulverbund

- ✓ Mehrere RZs, Georedundanz, SaaS
- ✓ Multi-Instance und DB-Cluster

# Roadmap des Rollout Flows

Ausblick: von der Idee bis zum Shibboleth IdP mit integriertem Self-Service-Portal

**Phase I**
100% abgeschlossen

Ausrollen bei Pilotkunden

**Phase II**
in Bearbeitung

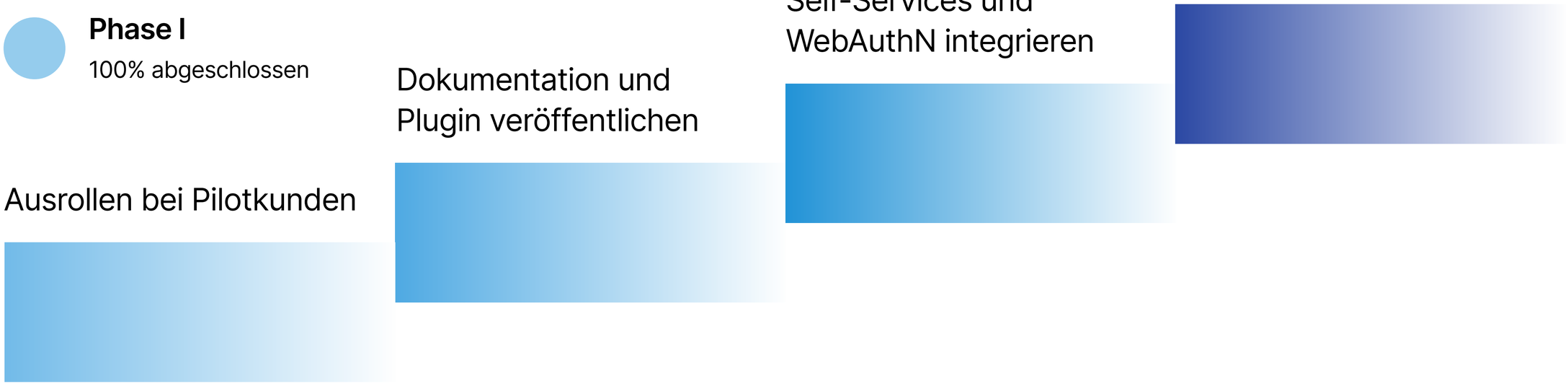
Dokumentation und Plugin veröffentlichen

**Phase III**
in Vorbereitung

Self-Services und WebAuthN integrieren

**Phase IV**
Ausblick

Kompletter Account Self-Service in Shibboleth



→https://www.ssystems.de/edumfa/rollout

# Fragen? Anregungen?

Sprechen Sie uns gerne an oder schreiben Sie uns!


**Harald Strack**

gf@ssystems.de



**Dr. Raoul Hentschel**

rhentschel@ssystems.de