Hochschule
München
University of
Applied Sciences

Unlocking the Future of (edu)MFA: Integrating Passkeys for Research and Education

Erwin Kupris
Florian Ritterhoff
Steffen Hofmann (FU Berlin)
Thomas Schreck

32. DFN-Konferenz „Sicherheit in vernetzten Systemen“

12.02.2025

Agenda

- Motivation
- Grundlagen
- Herausforderungen von MFA in R&E
- eduMFA
- Erste Erkenntnisse
- Zukünftige Arbeiten

Motivation

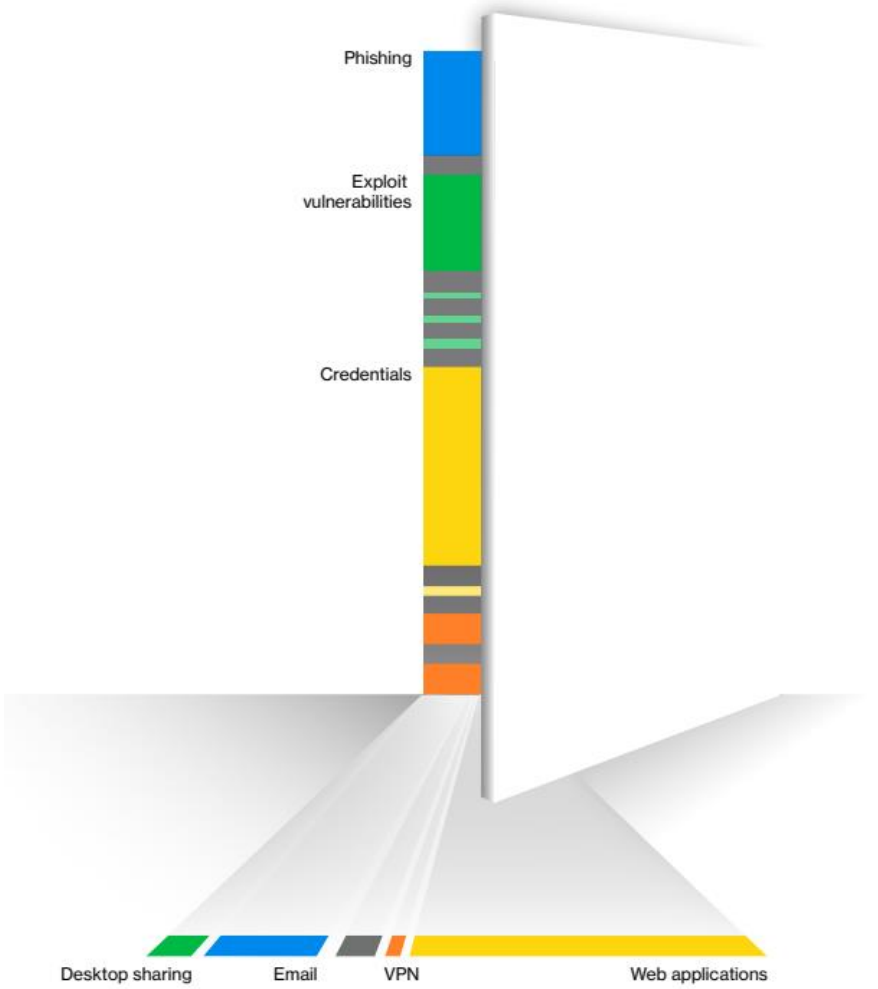
- Angriffe auf R&E nehmen zu
- Passwörter häufig der Grund
- Traditionelle MFA-Methoden sind ok, aber haben einige Probleme
- FIDO2 ermöglicht passwortlose MFA!

Educational Services (NAICS 61)	
Frequency	1,780 incidents, 1,537 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Miscellaneous Errors represent 90% of breaches
Threat actors	External (68%), Internal (32%) (breaches)
Actor motives	Financial (98%), Espionage (2%) (breaches)
Data compromised	Personal (83%), Internal (20%), Other (18%), Credentials (9%) (breaches)
What is the same?	The same three patterns dominate this vertical as last year. External actors stealing Personal data accounts for the majority of breaches.
Summary	Errors of various types committed by internal actors and Extortion from external threat actors continue to constitute the curriculum of this industry.

Source: Verizon 2024 Data Breach Investigations Report

Motivation

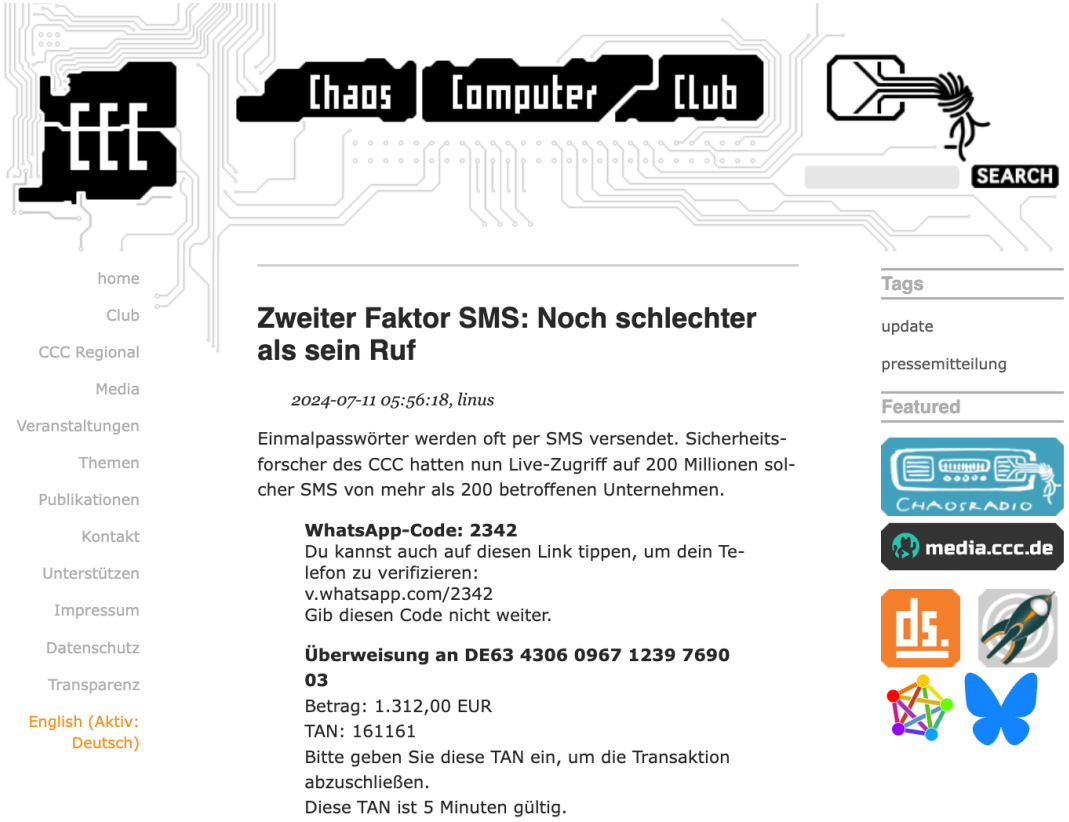
- Angriffe auf R&E nehmen zu
- Passwörter häufig der Grund
- Traditionelle MFA-Methoden sind ok, aber haben einige Probleme
- FIDO2 ermöglicht passwortlose MFA!



Source: Verizon 2024 Data Breach Investigations Report

Motivation

- Angriffe auf R&E nehmen zu
- Passwörter häufig der Grund
- Traditionelle MFA-Methoden sind ok, aber haben einige Probleme
- FIDO2 ermöglicht passwortlose MFA!



Source: Chaos Computer Club https://www.ccc.de/de/updates/2024/2fa-sms

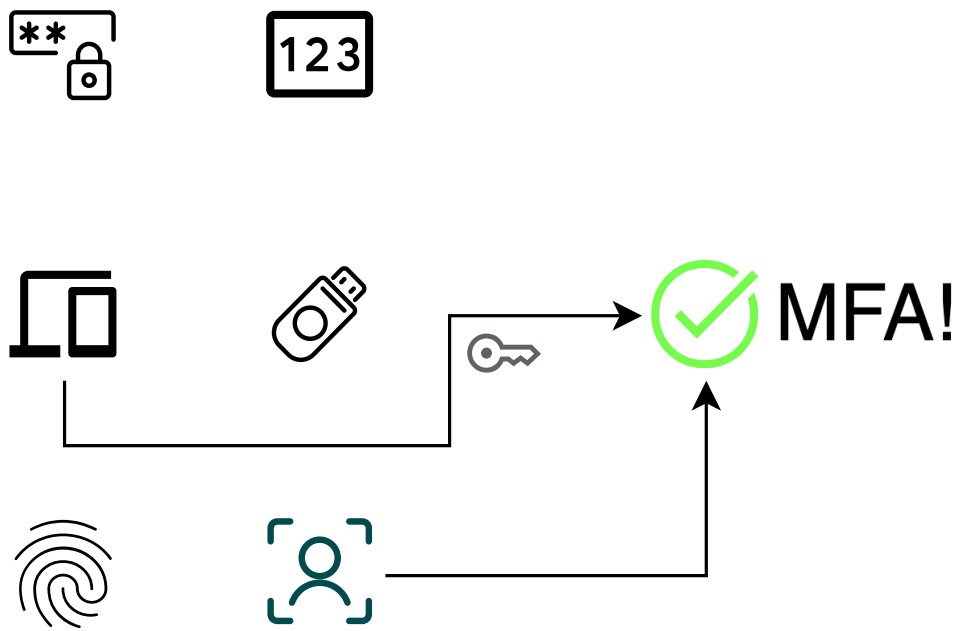
Motivation

- Angriffe auf R&E nehmen zu
- Passwörter häufig der Grund
- Traditionelle MFA-Methoden sind ok, aber haben einige Probleme
- FIDO2 ermöglicht passwortlose MFA!

Source: FIDO Figma UI Kit https://www.figma.com/@fido

Grundlagen: Multi-Faktor-Authentifizierung

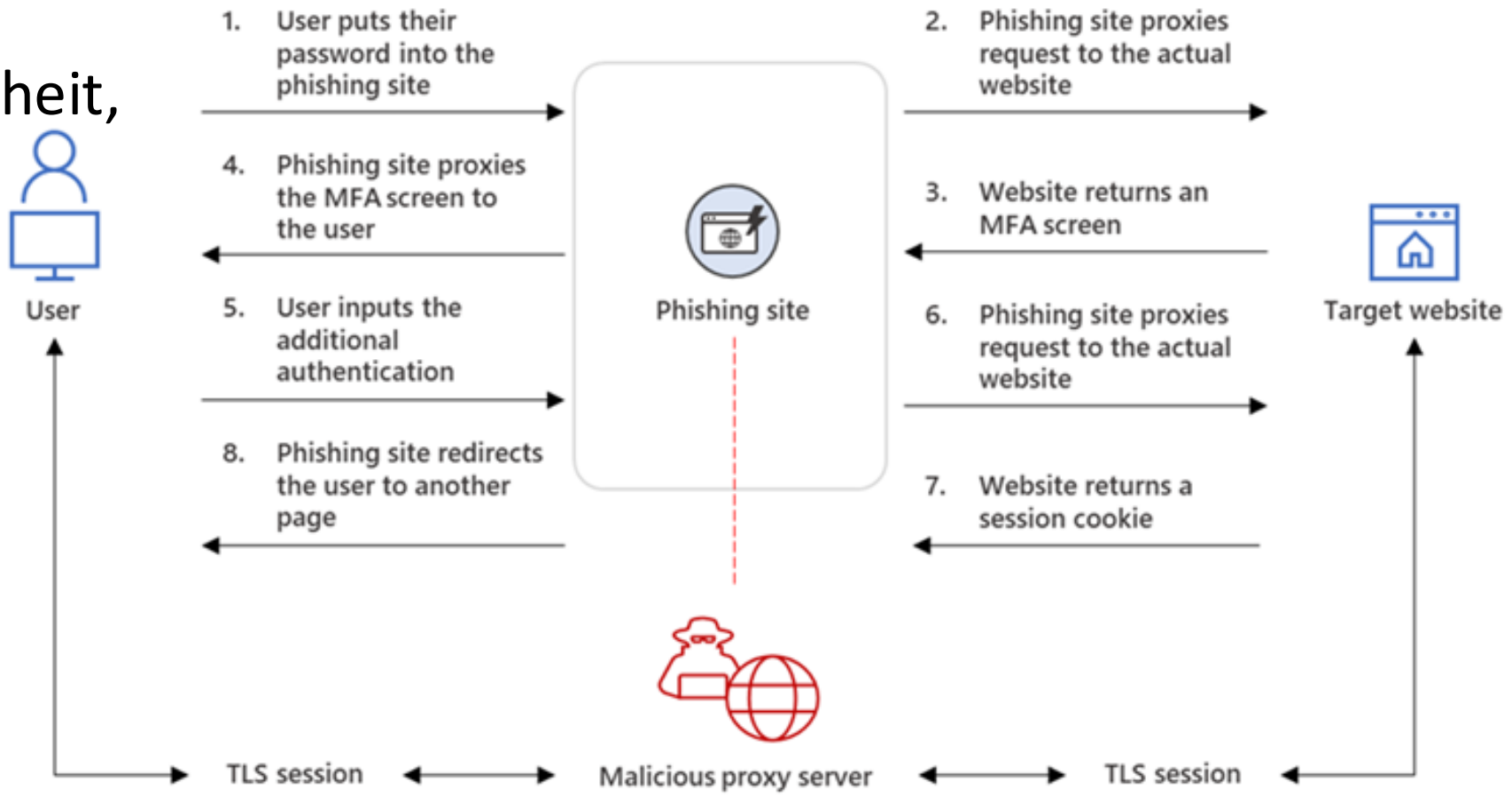
- Faktoren für Authentifizierung
  - Wissen (Something you know)
  - Besitz (Something you have)
  - Biometrie (Something you are)
- Zwei-Faktor != Zwei Schritte



Grundlagen: Traditionelle MFA-Methoden

Verbessern die Sicherheit,
aber es gibt Angriffe:

- SIM-Swapping
- Phishing noch möglich

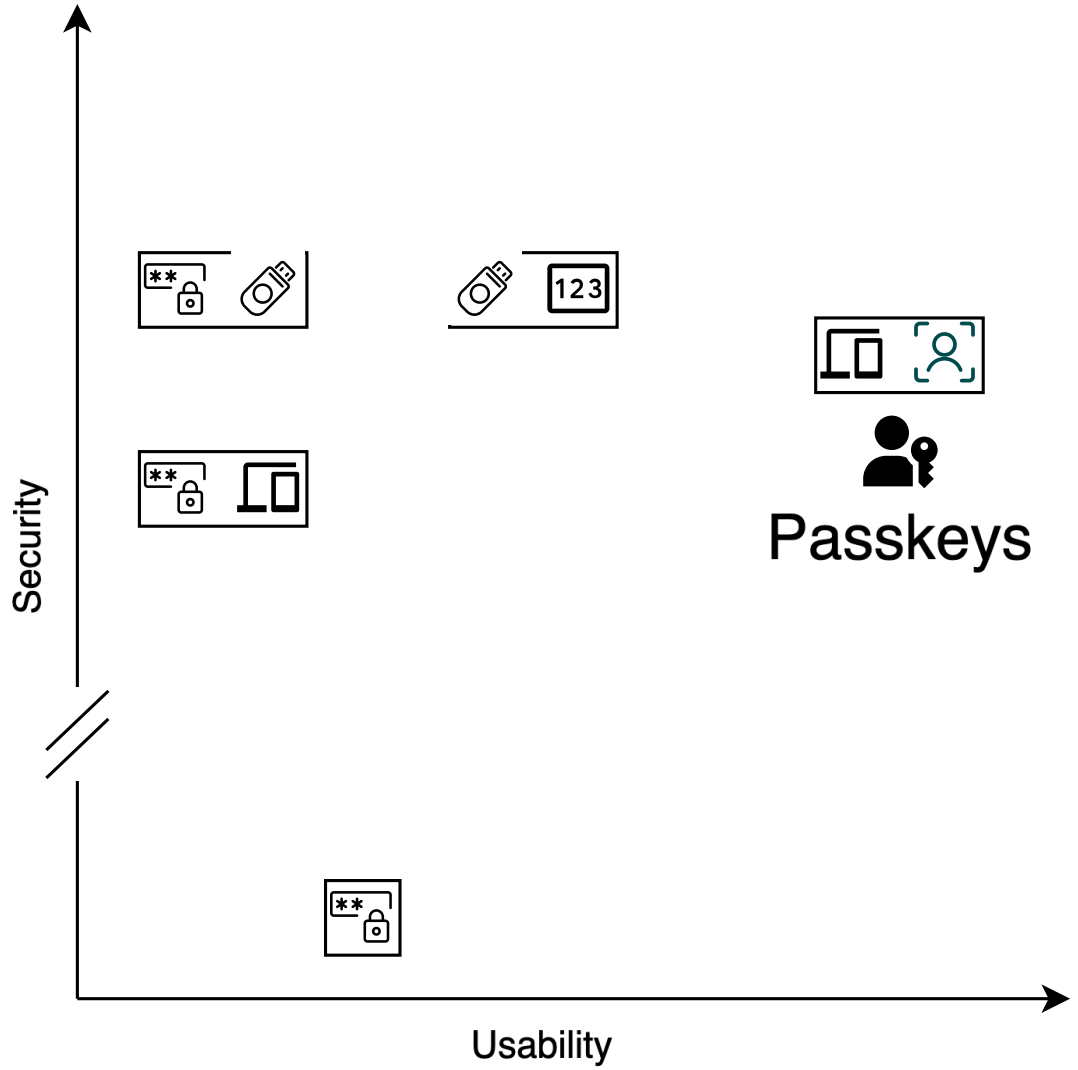


Source: https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

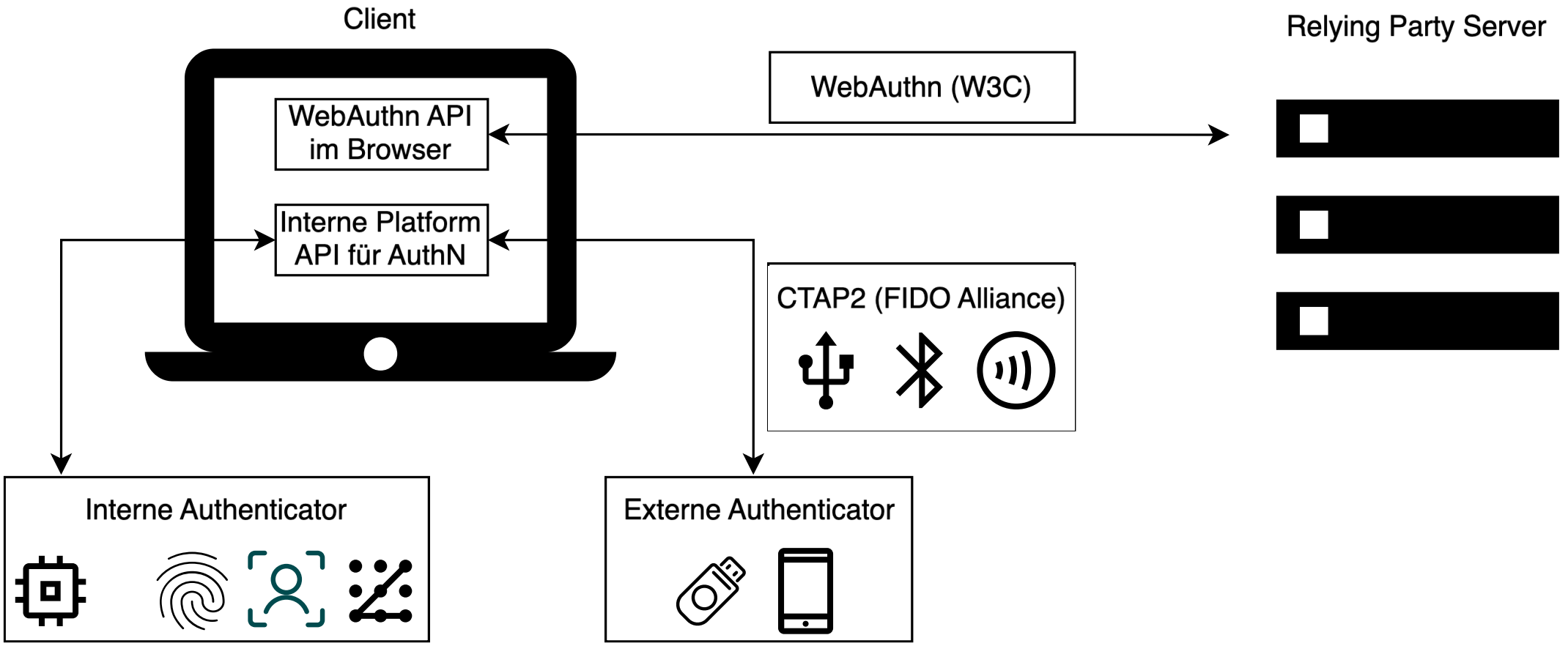
Grundlagen: Traditionelle MFA-Methoden

Nutzbarkeit eingeschränkt

- Extra Gerät
- Dauert länger
- Recovery
- …



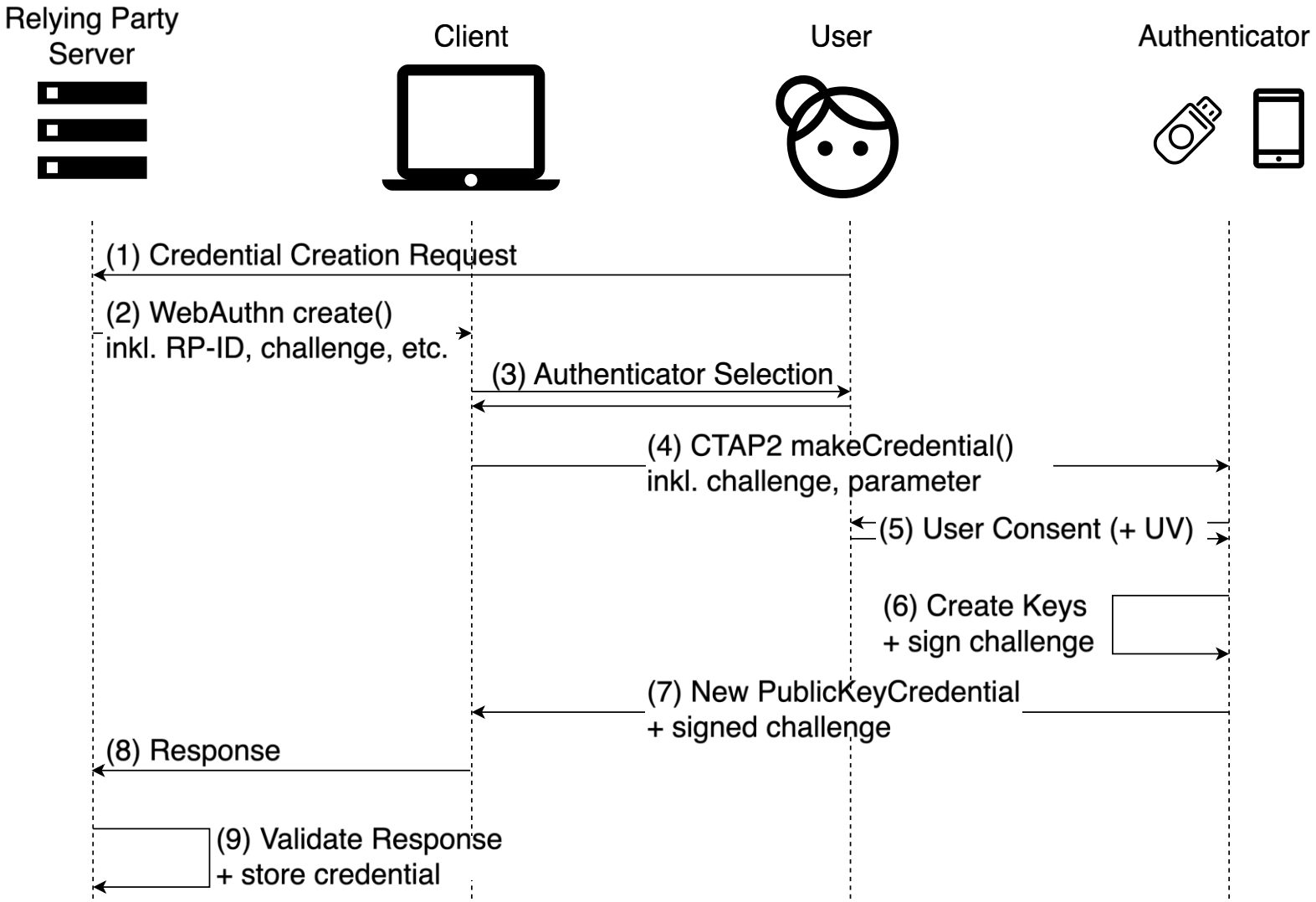
Grundlagen: FIDO2



Grundlagen: FIDO2

- Challenge-Response Verfahren
- Asymmetrische Kryptographie
- User Consent immer notwendig
- 2. Faktor über User Verification
  - PIN
  - Biometrische Merkmale
- Resistent gegen Phishing-Angriffe

Grundlagen: FIDO2



Grundlagen: Passkeys

Client-Side Discoverable:

- Ist auf dem Authenticator gespeichert
- Kann von Browser gefunden werden (Conditional Mediation)
- → Usernameless MFA!

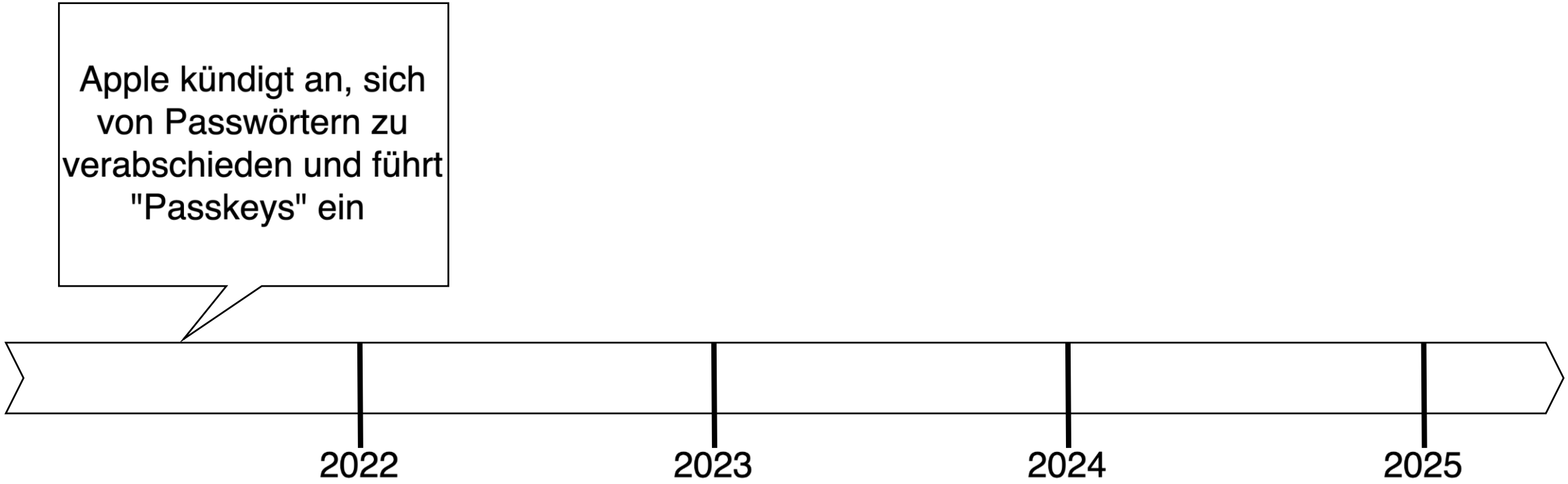
Entweder syncable oder device-bound:

- Syncable:
  - Apple via iCloud Keychain
  - Android via Google Cloud
- Device-bound:
  - Windows (zur Zeit)
  - Sicherheitsschlüssel

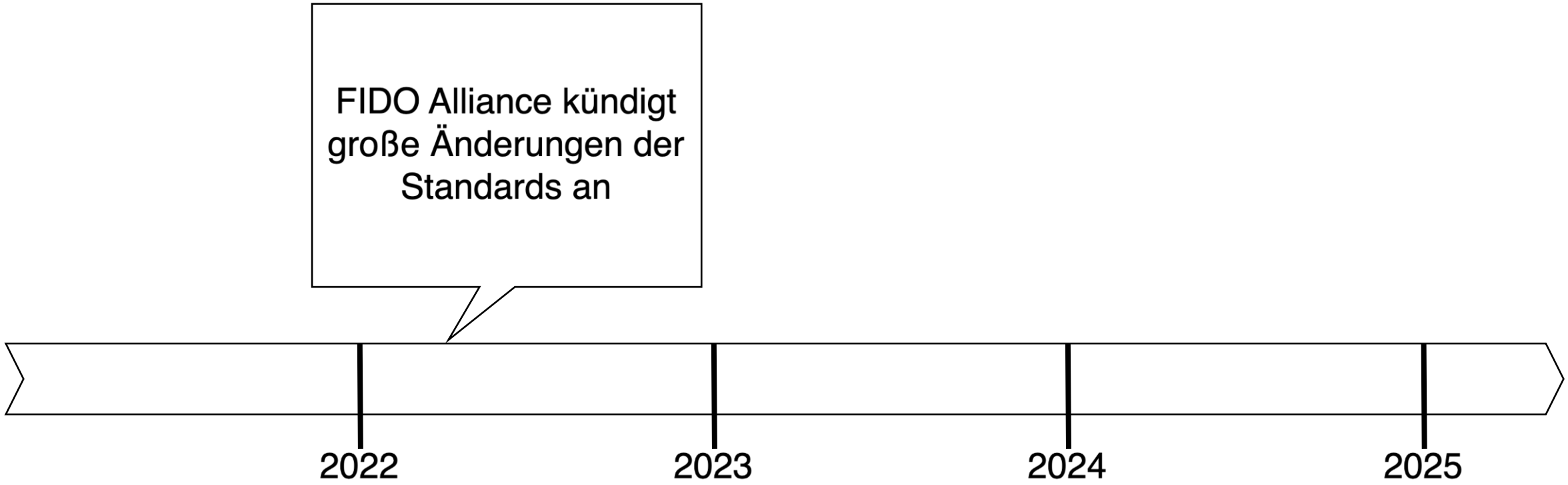
Herausforderungen von MFA in R&E

1. Unterschiedliche Nutzergruppen
2. Verschiedenste Endgeräte
3. Diverse Applikationen und Websites
4. Unterschiedlich große Institutionen
5. Last fluktuiert über das Jahr stark
6. Shibboleth IdP weit verbreitet

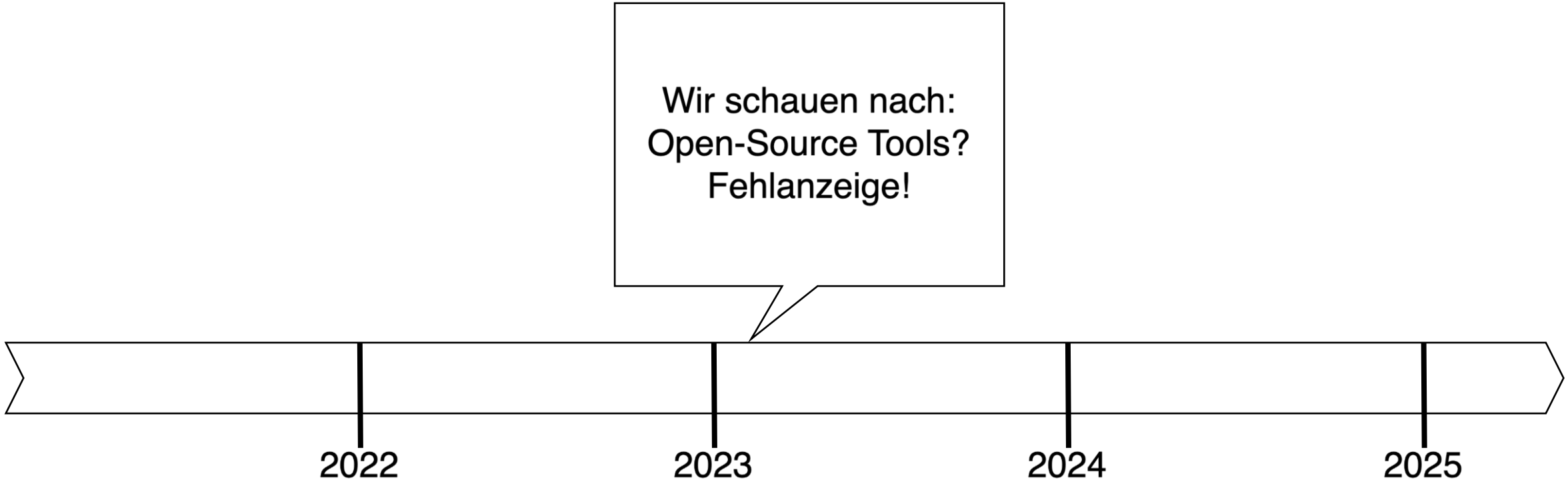
Timeline von eduMFA und Passkeys



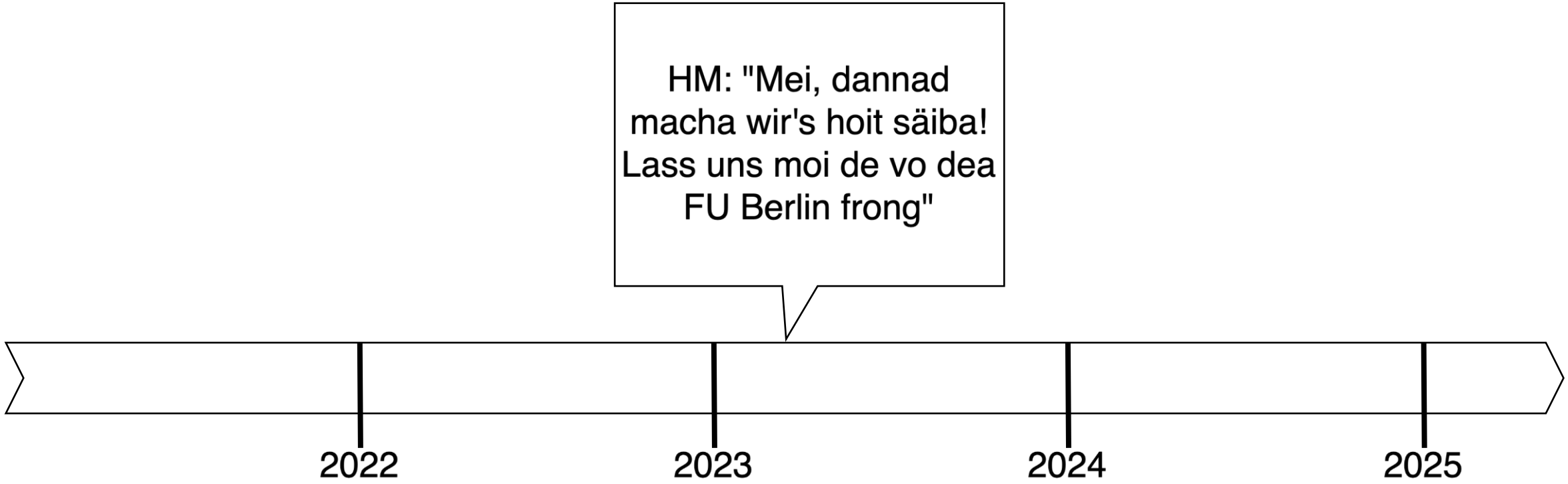
Timeline von eduMFA und Passkeys



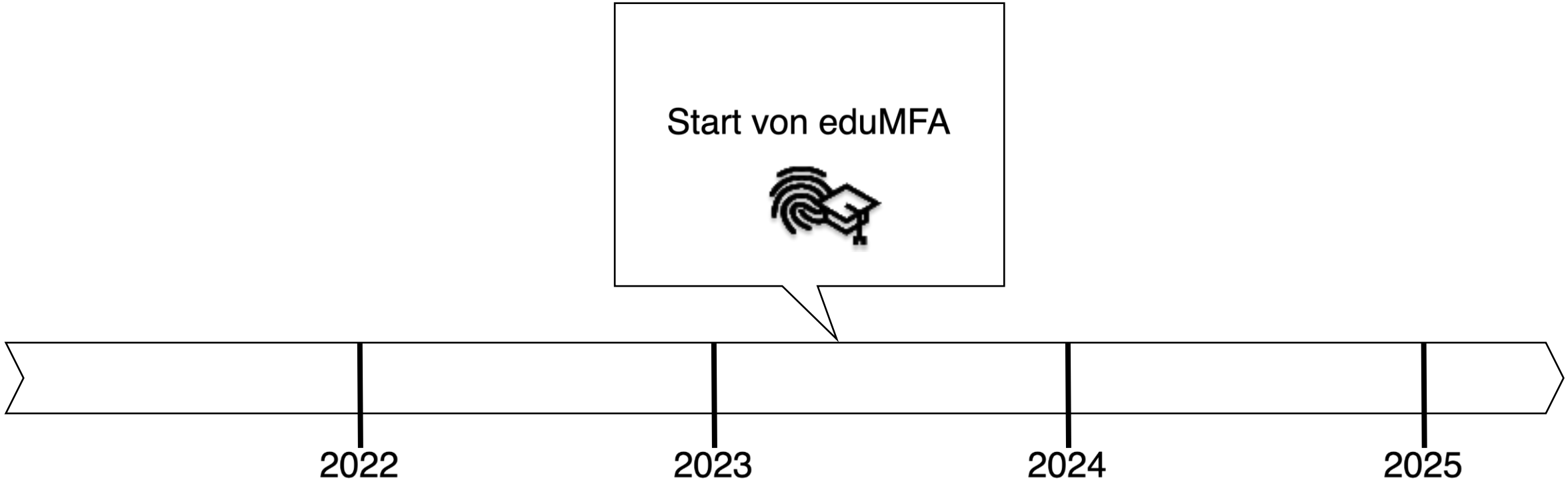
Timeline von eduMFA und Passkeys



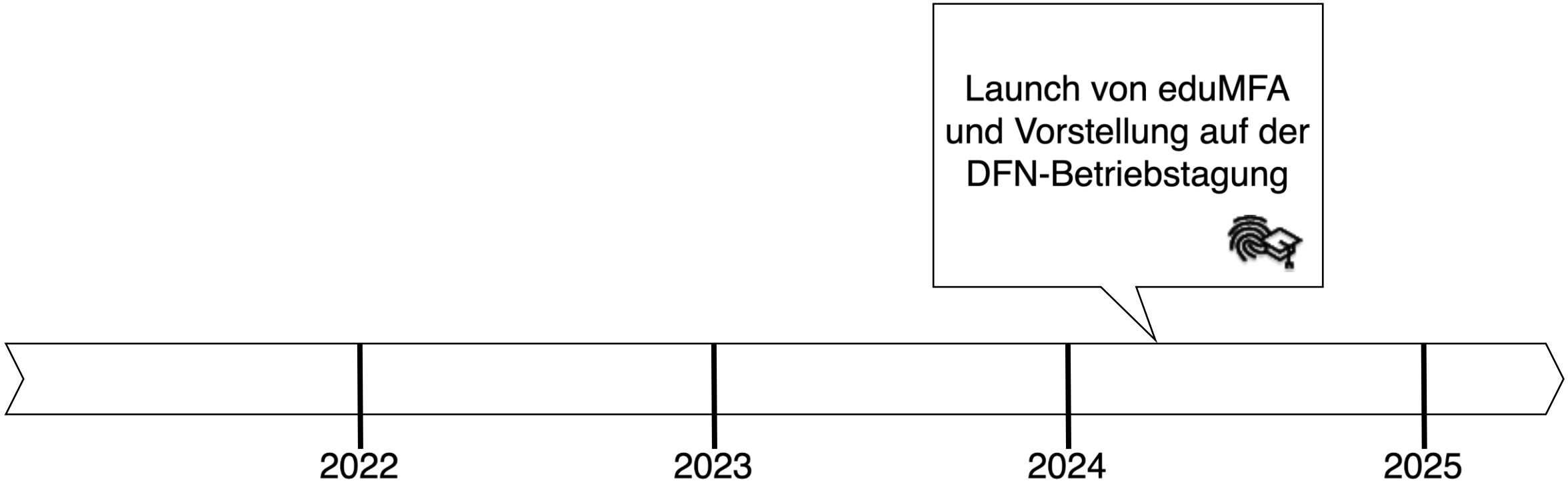
Timeline von eduMFA und Passkeys



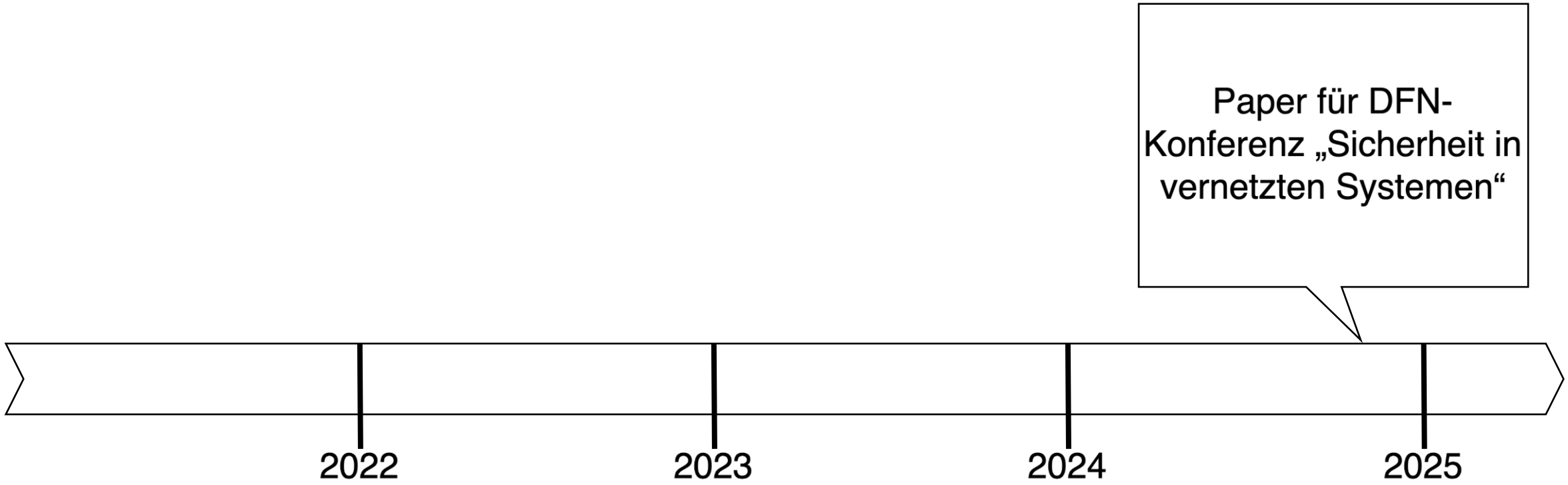
Timeline von eduMFA und Passkeys



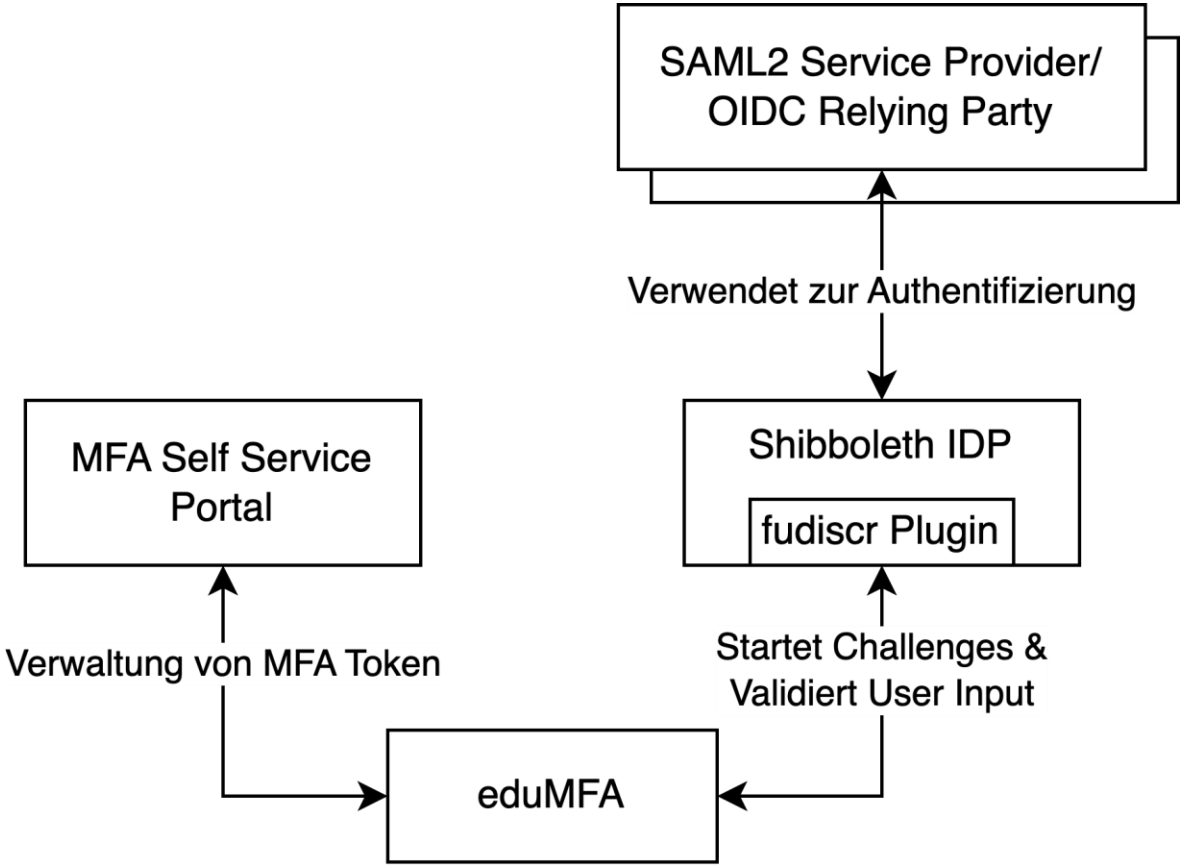
Timeline von eduMFA und Passkeys



Timeline von eduMFA und Passkeys



eduMFA Architektur



eduMFA Anpassungen für Passkeys

eduMFA

- Integration von Passkeys
- Generierung von Challenges ohne einen Nutzer zu kennen
- Neue Policys für Passkeys, Passwordless und Usernameless Login

Shibboleth

Inkl. fudiscr Plugin

- Shibboleth Login-Views unterstützen Passkeys und Conditional Mediation
- fudiscr unterstützt nun Passkeys und den Login ohne Nutzernamen

Integration von Passkeys in eduMFA

- Aufwand klein halten → Anpassung von vorhandenem Code
- Usernameless: Jeder Aufruf der Loginseite verursacht Transaktionen
  → Ziel DB Last klein halten
  → Generierung von Challenges auf Basis von JWT → Stateless!
- Sammeln von möglichst vielen Infos
  → Nicht alle Browser liefern gleich viel Infos
- Python leider eher langsam → Container + Scaling
- Dependency Updates

fudiscr Anpassungen für Passkeys

- Bei Challenge-Generierung für Passkeys:
  - Keine Nutzerinfos vorhanden
  - Aber: Sehr wenige Informationen notwendig

→ Statisches Hinterlegen von einigen Default Werten in Shibboleth

- Benutzername & Passwort + Passkeys sollen parallel funktionieren
  → „Subflow" von Standard Login + Zwischenscreen für "Unknown" Passkey

- Erkennung von User notwendig
  → Speicherung von Username bei Rollout & Extraktion bei Authentifizierung
  → Realm-Funktionalität wieder gegeben

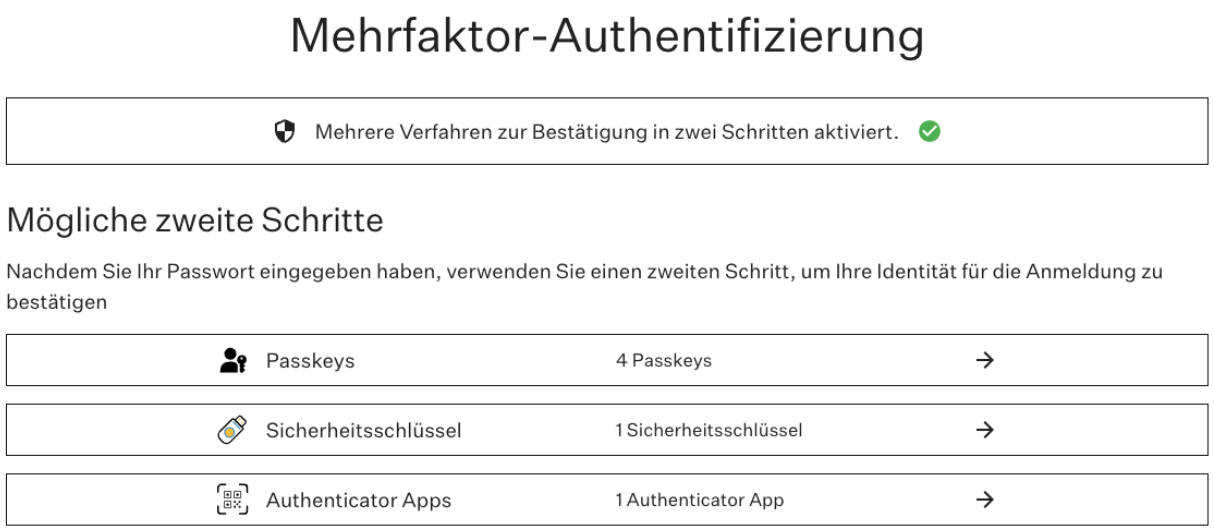
- Nicht alle Browser können Conditional Mediation → Manueller Button

UI Anpassungen

Diverse Anpassungen für Verwendung von Passkeys:

- Integration in Shibboleth Login Maske
- Unknown Passkey Screen
- Entwicklung von eigenem Portal, für größtmögliche Flexibilität und Optionen
  - FIDO UX Best Practices
  - Validiert durch UX und Design Profs

Self-Service UI



Herausforderungen von MFA in R&E

1. Unterschiedliche Nutzergruppen
2. Verschiedenste Endgeräte
3. Diverse Applikationen und Websites
4. Unterschiedlich große Institutionen
5. Last fluktuiert über das Jahr stark
6. Shibboleth IdP weit verbreitet

Konsistente und gute UX für alle Nutzergruppen + Accessibility Studie kommt

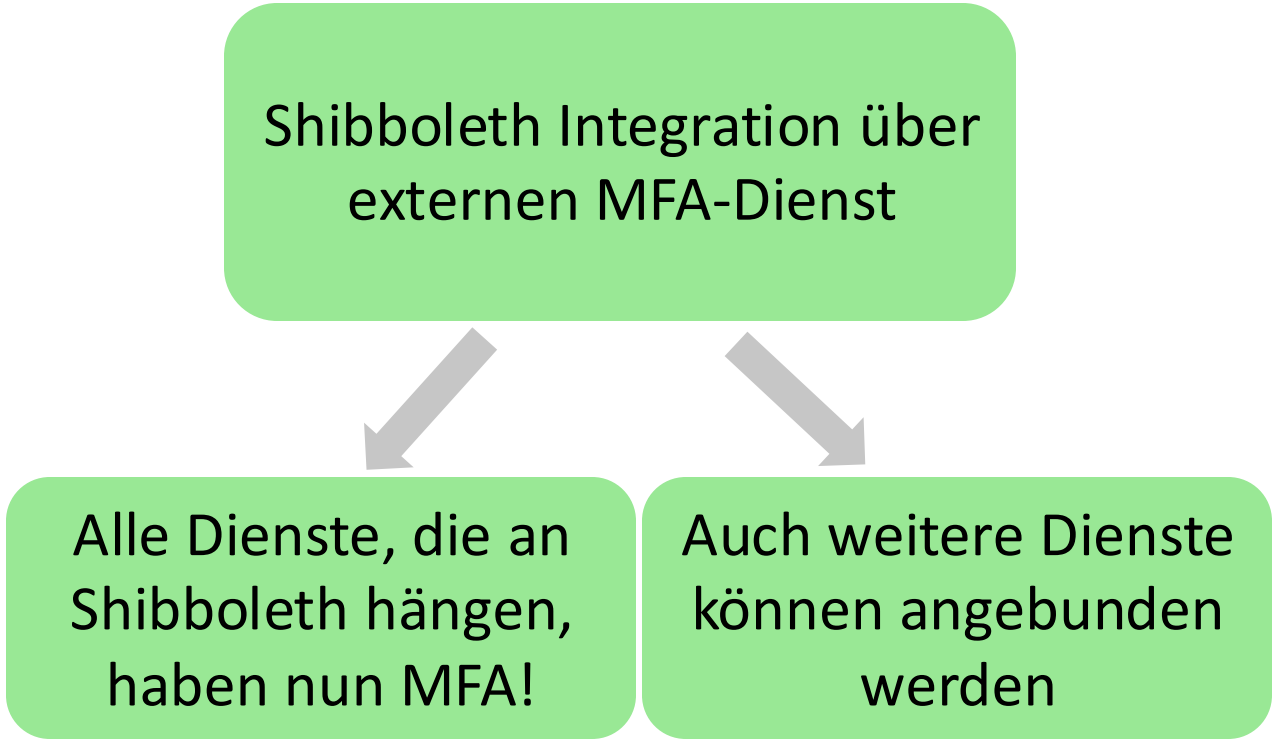
Herausforderungen von MFA in R&E

1. Unterschiedliche Nutzergruppen
2. Verschiedenste Endgeräte
3. Diverse Applikationen und Websites
4. Unterschiedlich große Institutionen
5. Last fluktuiert über das Jahr stark
6. Shibboleth IdP weit verbreitet

Aktuelle Geräte unterstützen FIDO2, sonst YubiKeys oder PW-Manager

Herausforderungen von MFA in R&E

1. Unterschiedliche Nutzergruppen
2. Verschiedenste Endgeräte
3. Diverse Applikationen und Websites
4. Unterschiedlich große Institutionen
5. Last fluktuiert über das Jahr stark
6. Shibboleth IdP weit verbreitet



Herausforderungen von MFA in R&E

1. Unterschiedliche Nutzergruppen
2. Verschiedenste Endgeräte
3. Diverse Applikationen und Websites
4. Unterschiedlich große Institutionen
5. Last fluktuiert über das Jahr stark
6. Shibboleth IdP weit verbreitet

Deployment via Docker und Kubernetes: Scalability, Load-Balancing, Rolling Upgrades, etc.

Erste Erkenntnisse - Enrollment

- Security Key PIN:
    - Muss (je nach Browser) vorkonfiguriert sein
    - z.B. via YubiKey Manager
- Verhalten von Geräten/Browsern unterscheidet sich
- Relying Party ID muss zu Use-Cases passen
- Fehler abfangen, sonst:
    - Unbrauchbare Credentials
    - Ausgesperrte User
- → Self-Service Portal + Fallback Methoden

Erste Erkenntnisse - Nutzung

- Manche Apps nutzen alte, eingebettete Browser ohne (aktuellen) FIDO2 Support

- Use-Cases beachten und prüfen:
  - Studierende in Laboren?
  - Studierende bei Prüfungen?

Erste Erkenntnisse - Löschen

- Wird ein Passkey von einer Website gelöscht, muss dieser auch von dem Authenticator gelöscht werden!

  → Eine passende API wurde vorgeschlagen

- Unter Windows 10 kann ein Passkey nur mit Admin Rechten via Konsole gelöscht werden

Erste Erkenntnisse - Usability von Passkeys

- Passkeys auf Platform Authentikatoren haben signifikant höhere:
  - Nutzbarkeit
  - Akzeptanz
  - Performance
- Geteilte Meinungen zur Verwendung privater Geräte
  - Studierende finden es super und sind es gewohnt
  - Lehrendes Personal ist es eher gewohnt
  - Sonstiges Personal ist häufig dagegen

Zukünftige Arbeiten

- Studie zu Usability und Akzeptanz -> Done!
- Langzeitstudie begleitend zur flächendeckenden Einführung -> Geplant!
- Studie zur Accessibility von MFA-Methoden -> Geplant!
- Erweiterungen von eduMFA -> ongoing!
  - Authenticator App
  - Anbindung an EntraID
  - WebAuthn Level 3

Fazit

- Passkeys verbinden Sicherheit mit Nutzbarkeit
  - Aber: Es gibt noch einzelne Fallstricke
  - Fallback MFA-Methoden sind wichtig

- eduMFA legt die Grundlage für:
  - sichere
  - nutzbare
  - zukunftsfähige

Multi-Faktor-Authentifizierung
an R&E Institutionen

Großes Danke an die eduMFA Projektpartner!

HM Hochschule München University of Applied Sciences

FREIE UNIVERSITÄT BERLIN

UNIVERSITY OF BAMBERG OTTO-FRIEDRICH-UNIVERSITÄT BAMBERG PAT. UNIV. BAMBERG

DAASI International

GWDG Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen