eduMFA

Aktueller Stand und geplante Entwicklungen

Agenda

- Warum eduMFA?
- Status Entwicklung
- eduMFA und Passkeys
- Migration zu eduMFA
- eduMFA Support
- Future Work

Warum eduMFA? … viele Ideen

- Fokussierung der Funktionen auf Hochschulen und andere wissenschaftlichen Einrichtungen
- Schaffung einer gemeinsamen Plattform für IT-Sicherheit
- Breite Entwicklerbasis
- Langfristiges Commitment
- Aufbau eines zentralen Supports im Wissenschaftsnetz
- Vorbereitung für einen Cloud-Dienst für kleine Hochschulen (Managed Service)
- Enger Austausch mit Shibboleth-Konsortium

eduMFA Projektpartner

Status eduMFA Entwicklung

- Quellcode: https://edumfa.io oder https://github.com/eduMFA/eduMFA
- Fork von privacyIDEA 3.9.2
- Erste WebAuthn-Erweiterung: Unterstützung von Passkeys
- Kleine Verbesserungen in der API
- Erweiterung SMS-Token mit Benachrichtigung per User

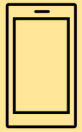
eduMFA und Passkeys

Warum Passkeys?

Passwörter

- Anfällig für Phishing
- Unvereinbarkeit von Nutzbarkeit und Sicherheit

Etablierte MFA-Methoden



- Verbesserte Sicherheit, aber einige Sicherheitsprobleme bestehen
- Nutzbarkeit oft eingeschränkt

Passkeys

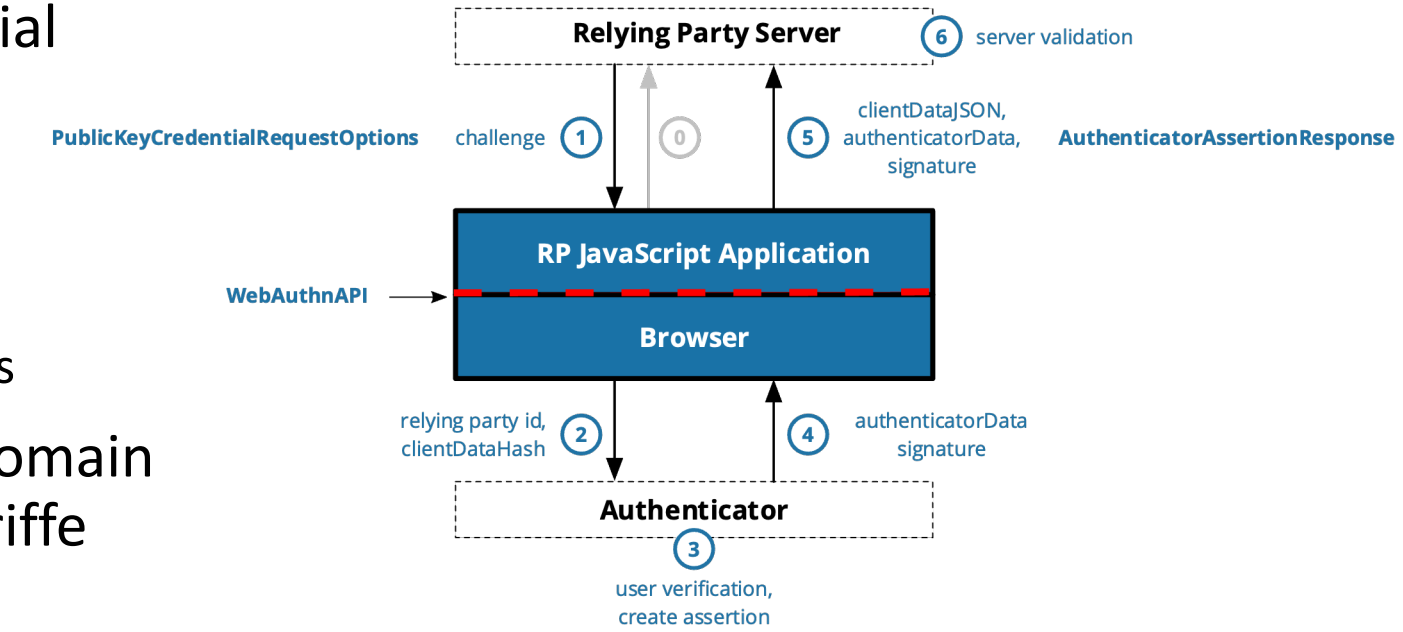
- Sehr sicher, weil resistent gegen Phishing-Angriffe
- Erhöhte Nutzbarkeit

Was sind Passkeys genau?

= WebAuthn (Multi-Device) Client-Side Discoverable Credentials

WebAuthn (Multi-Device) Client-Side Discoverable Credentials

- W3C Standard PublicKeyCredential
- Challenge-Response Verfahren
- Authenticator:
  - Hardware-Sicherheitsschlüssel
  - Moderne Geräte, z.B. Smartphones
- Eigenes Schlüsselpaar für jede Domain
  -> Resistent gegen Phishing-Angriffe

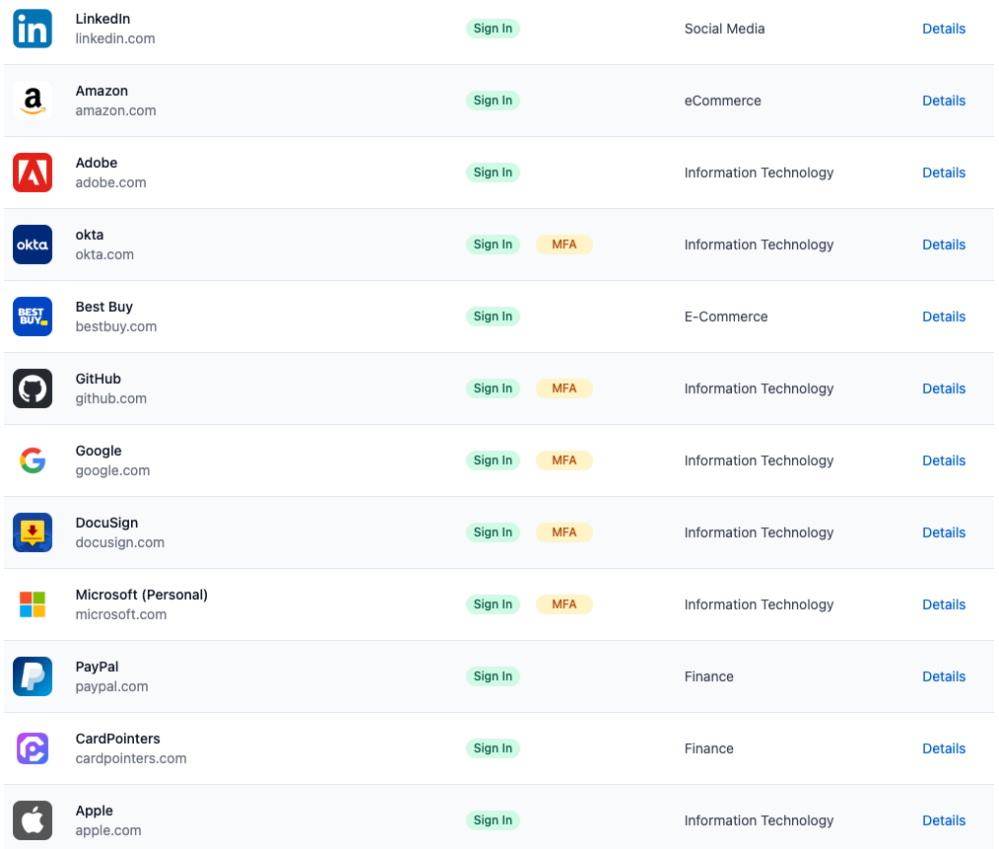


WebAuthn (Multi-Device) Client-Side Discoverable Credentials

- Multi-Device:
  - Können zwischen kompatiblen Geräten synchronisiert werden (Cloud-Account)
  - Alternative: Device-Bound Passkeys, z.B. Windows oder Sicherheitsschlüssel
- Client-Side Discoverable:
  - Credential ist auf dem Authenticator gespeichert
  - Zusätzlich gespeichert: Nutzername, Relying Party ID (Domainname)
  - MFA in einem Schritt, ohne Passwort und Nutzernamen einzugeben

Status Passkeys

Immer mehr große Seiten bieten Passkeys an, siehe https://passkeys.directory



LinkedIn linkedin.com	Sign In		Social Media	Details
Amazon amazon.com	Sign In		eCommerce	Details
Adobe adobe.com	Sign In		Information Technology	Details
okta okta.com	Sign In	MFA	Information Technology	Details
Best Buy bestbuy.com	Sign In		E-Commerce	Details
GitHub github.com	Sign In	MFA	Information Technology	Details
Google google.com	Sign In	MFA	Information Technology	Details
DocuSign docusign.com	Sign In	MFA	Information Technology	Details
Microsoft (Personal) microsoft.com	Sign In	MFA	Information Technology	Details
PayPal paypal.com	Sign In		Finance	Details
CardPointers cardpointers.com	Sign In		Finance	Details
Apple apple.com	Sign In		Information Technology	Details

OS- und Browser-Support nimmt stetig zu, siehe https://passkeys.dev/

Capability	Android	Chrome OS	iOS/iPadOS	macOS	Ubuntu	Windows
Synced Passkeys	✓ v9+	📅 Planned [1]	✓ v16+	✓ v13+ [2]	✗ Not Supported	📅 Planned [1]
Browser Autofill UI	✓ Chrome 📅 Edge ✗ Firefox	📅 Planned	✓ Safari Chrome Edge Firefox	✓ Safari Chrome Firefox [4] 📅 Edge	✗ Not Supported	✓ Chrome [3] Firefox [4] 📅 Edge

Limitations von Passkeys

- Vertrauen in Cloud-Provider
- Synchronisierung zwischen Cloud-Providern noch nicht möglich
- User müssen aufgeklärt werden!
- Bisher nur Web -> andere Protokolle (IMAP, SMTP)

eduMFA Anpassungen für Passkeys

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

Inkl. fudiscr Plugin

- Shibboleth Login-Views unterstützen Passkeys und Browser Autofill UI
- fudiscr unterstützt nun Passkeys und den Login ohne Nutzernamen

Shibboleth-Plugin fudiscr

- 1.x Versionen für IdP 4, 2.x Versionen für IdP 5
- Ab 01.04.2024 „current“ Versionen 1.4.0/2.0.0
  - mit eduMFA-Client
  - mit Passkeys-Unterstützung
- EOL Shibboleth IdP 4 Ende 2024
  - EOL fudiscr Version 1.x parallel Ende 2024
  - Nur noch Bugfixes in 1.x
- Support für privacyIDEA bleibt bestehen

Migration zu eduMFA

- Notwendige Upgrade-Schritte
  - Update auf PrivacyIDEA 3.9.2
  - Gemäß READ_BEFORE_UPDATE.md unter https://github.com/eduMFA/eduMFA/
- Verfügbare Installationsmethoden:
  - Ubuntu Packages für 20.04 LTS (Focal) und 22.04 LTS (Jammy)
  - Docker-Examples
  - PyPI/pip mit Python 3.6+

Austausch und Support zu eduMFA

- Mail an edumfa@listserv.dfn.de
- Professioneller Support durch
  - DAASI International
  - GWDG (Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen)

Zukunft von eduMFA: Entwicklung

- Dependencies aktualisieren!!!
- Pentests durch externes Unternehmen
- eduMFA Authenticator App (wie Push-TAN)
  - Entwicklung durch GWDG
- API modernisieren
  - Zeitformate vereinheitlichen
  - aggregierte Informationen
  - Reduzierung API-Zugriffe
  - Janitor verbessern, z.B. alle Token eines Nutzers löschen
- Nebenprojekt: Moderne, nutzerfreundliche UI

Zukunft von eduMFA: Projekt

- Feedback aus der Community einbauen!
- Community vergrößern
- Partner holen