10. – 13.12.2018
Frankfurt am Main

Jan Lühr

Identitätsdiebstahl ade!

WebAuthn: Smartphone & Biometrie

#ittage

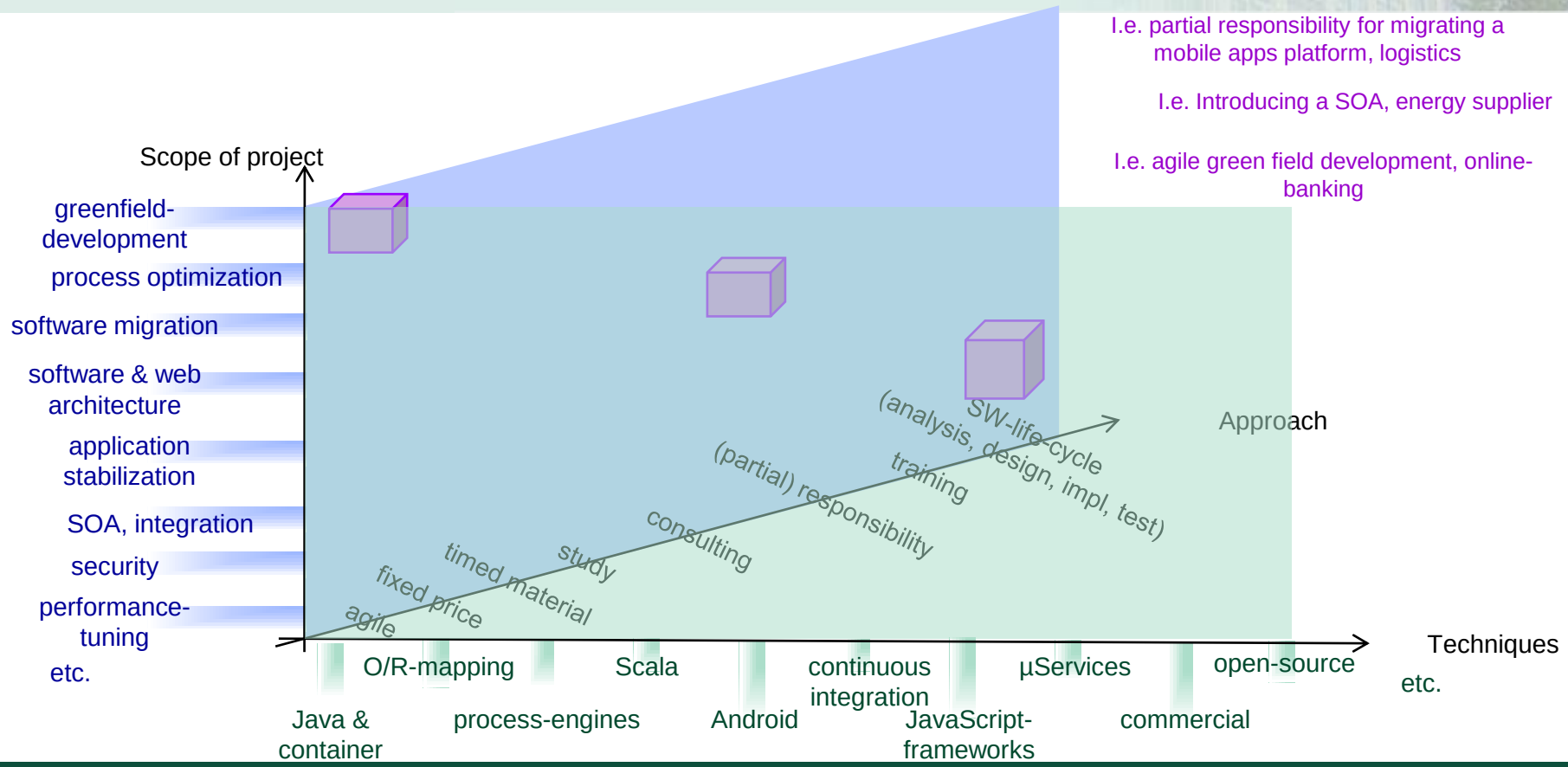
Agenda

Über mich

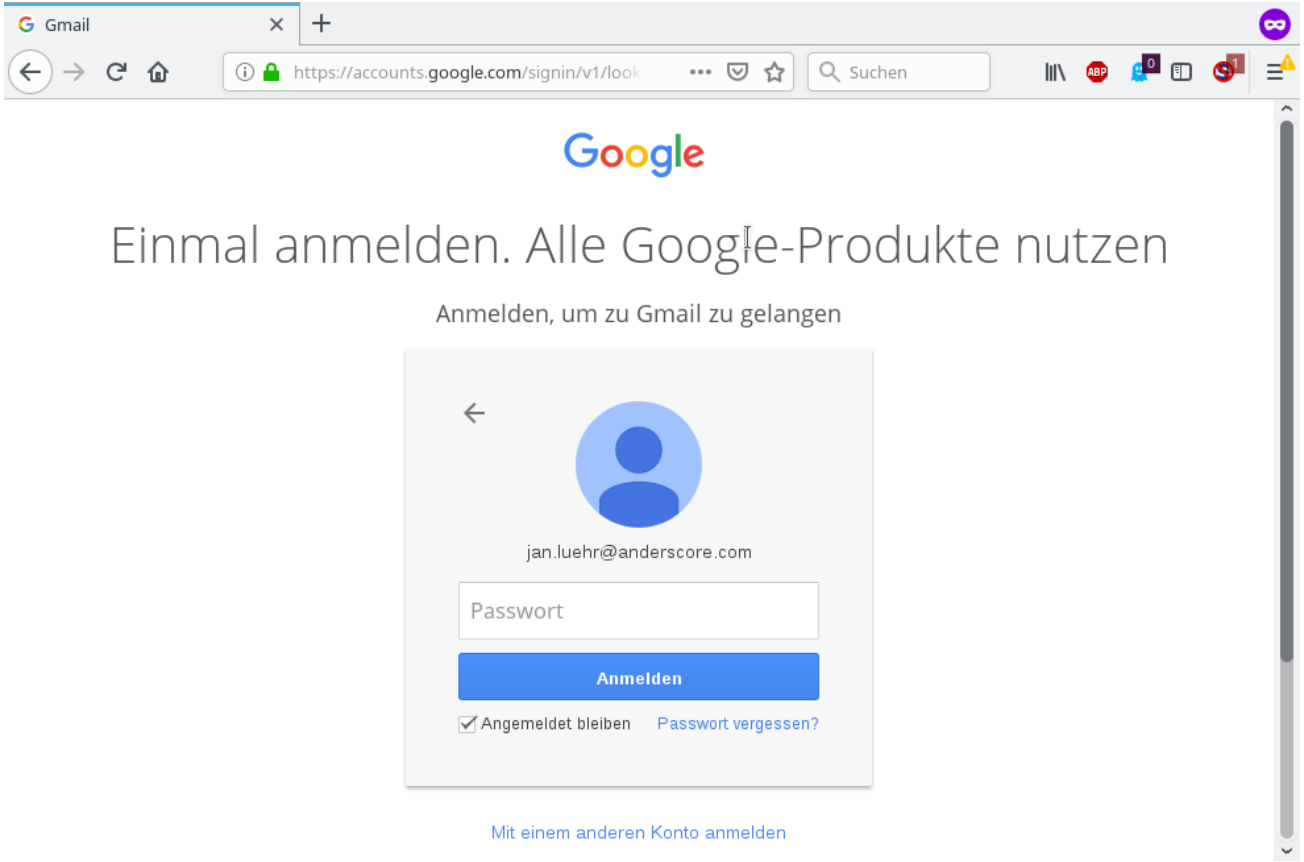
Jan Lühr

- B. Sc., Computer Science
- Senior Software Engineer & Architect
- anderScore seit 2007
- Fokus
  - Software Development
  - Pragmatic Architect
  - Network- and Security-Techniques
  - IT-Trainer
  - Java, JavaScript, Ruby
- **Auf den IT-Tagen: Stand 12**
  - **Neben der Information an den Rolltreppen (Ebene 1)**

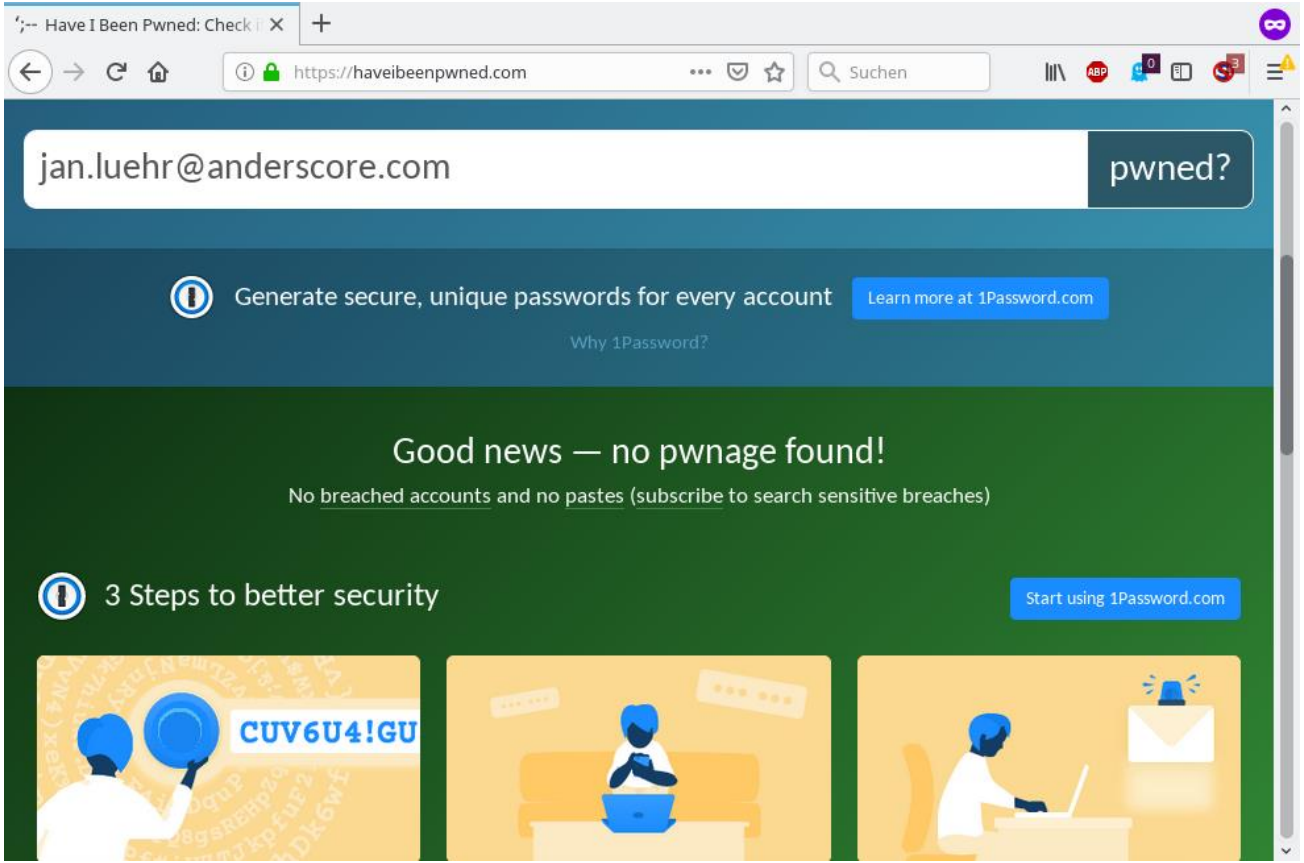
1. Unser Leistungsangebot



1. Motivation: Login



1. Motivation: Problemfall Passwort



1. Motivation: Angriff auf Web-Angebot

1. Angriff auf Web-Angebot: Nutzername & Kennwort gestohlen:
   - Einbruch in Server (**Datenreichtum**, p0wned, hack)
   - Gefälschte Version der Login-Seite im WWW (**phishing**)
2. Angreifer nutzt Zugangsdaten:
   - Zur Anmeldung am System des Opfers
   - Zur Anmeldung an **anderen Systemen** (identische Zugangsdaten)
3. Abwehr:
   - Phishing erschweren (z.T. schwer möglich)
   - Identity-Federation / Dienstleister nutzen (Datenweitergabe)
   - Ungewöhnliche Login-Versuche erkennen und sperren (sperrt z.T. legitime Nutzer)
   - Neben Kennwort **weitere Merkmale** fordern (z.B. Online-Banking: TAN-Nummer)

Weitere Merkmale fordern
Mehrfaktor-Authentisierung (MFA), Zwei-Faktor-Authentisierung (2FA)

2. MEHRFAKTOR-AUTHENTISIERUNG

2. Mehrfaktor-Authentisierung (MFA)

- Mehrere Merkmale zur Anmeldung – Kombination aus:
  1. Was jmd. **kennt – Wissen**
  2. Was jmd. **hat – Besitz**
  3. Was jmd. **ist – Biometrie**

- BSI IT-Grundschutz: *M 4.441 Multifaktor-Authentisierung für den Cloud-Benutzerzugriff:*

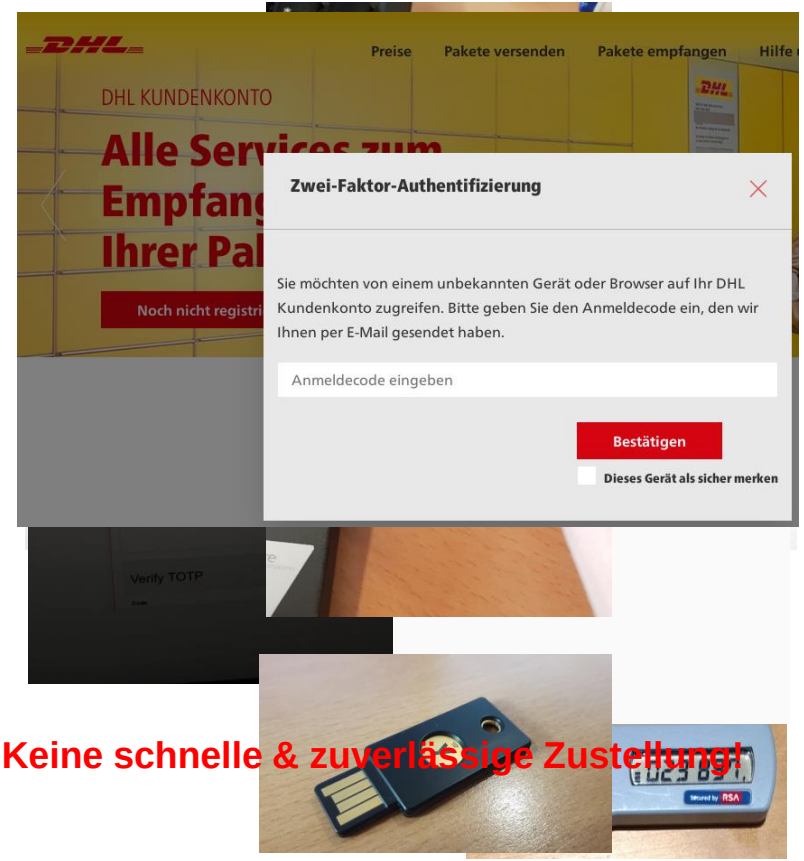
  „Eine sichere Lösung stellt hierbei eine Multifaktor-Authentisierung dar.
  Dabei sind mindestens zwei Faktoren für eine erfolgreiche Authentisierung erforderlich.“

2. Mehrfaktor-Authentisierung: Besitz

Was erfährt der Benutzer – User-Experience verbreiteter Verfahren:

- Typisch: Einmal-Passwörter (One-Time-Password – OTP)
  1. Papier-Liste (TAN)
  2. Challenge-Response-Verfahren / Event (iTan, Chip-Tan, HOTP)
  3. Zeitbasiert (TOTP)
  4. Push-Nachricht (mTan)

- Alternativ:
  1. Smartphone-App (z.B. Google Push)
  2. USB-Dongle (U2F, Smartcard)
  3. Smartcard
  4. Client-Zertifikate (TLS)



Keine schnelle & zuverlässige Zustellung!

2. MFA: Problematische Eigenschaften

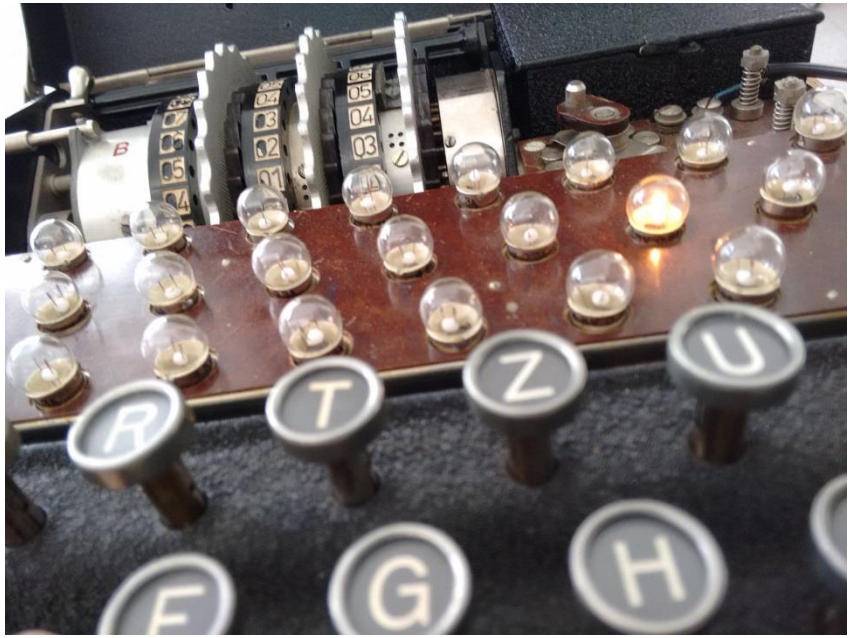
anderScore trust in competence

1. Schlechte User-Experience (UX):
   - Umständliches Handling
   - Token-Verlust: Kompliziertes Recovery

2. Unzureichender Schutz
   - Eingabe von TAN / OTP auf Phishing-Seite
   - Z.T. unsichere Plattform
     (SMS; RCE Android Media Subsystem)

3. Höhere Kosten
   - Zusatzhardware kostet Geld
   - Aufwendiges Deployment

4. Kein einheitlicher Standard
   - Proprietär: Software / Plug-Ins nötig
   - Meist Kaum Verbreitung im WWW



Ein neuer Standard für das World-Wide-Web

3. WEBAUTHN IM DETAIL

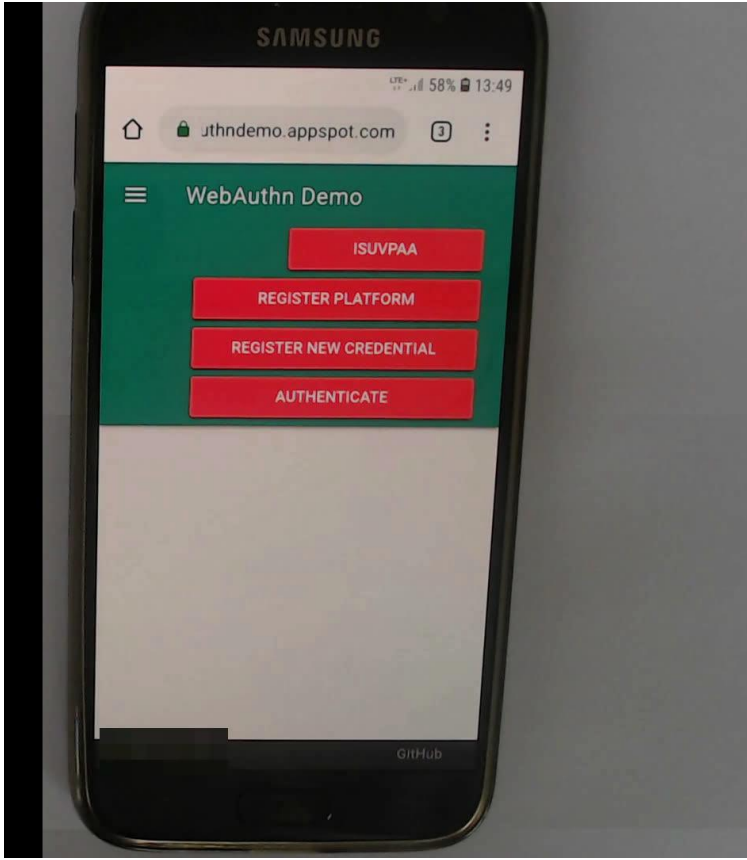
3. Web Authentication (WebAuthn)

- “Web Authentication: An API for accessing Public Key Credentials Level 1”
  - **W3C-Standard**, Status: Candidate Recommendation (08/2018)
  - Umgesetzt in Chrome, Firefox, MS Edge
  - Audit: Paragon Initiative Enterprises (08/2018)
    - Kryptographische Konventionen z.T. nicht befolgt (→ Schwächung)
    - Kein praktischer Angriff, **Nutzung empfohlen** (gegenüber 1-Faktor Kennwort)
- Technisch: Erweiterung / Standardisierung FIDO JavaScript U2F API
  - Public- / Private Key basierte Signatur: **Schutz vor Phishing; privater Key lokal gespeichert**
  - Erweiterung
    - Neue Verfahren (z.B. Fingerabdruck-Lesegeräte, **keine serverseitige Speicherung biometrischer Daten**)
    - Bestimmten Benutzer verifizieren (vorher: lediglich Präsenz eines Nutzers)

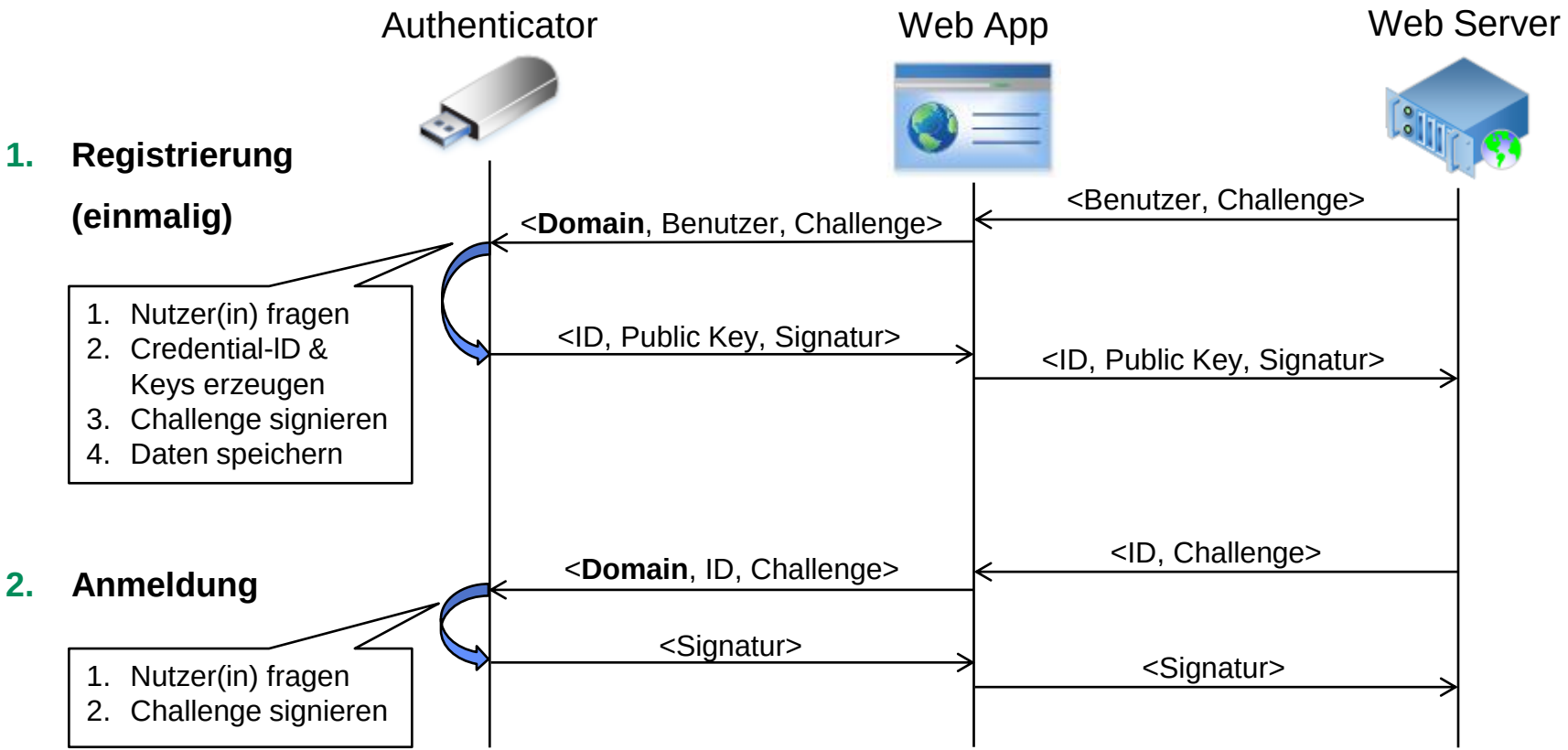
3. WebAuthn: User Experience (UX)

1. **Einmalige Registrierung des Geräts („Authenticator“)**

2. **Anmeldung**
   - **Ohne Kennwort**
   - (als weiterer Faktor)



3. WebAuthn: Technischer Ablauf



https://www.youtube.com/watch?v=lc7scxvKQOo

3. ANGRIFFSFORM: SOCIAL ENGINEERING

3. Angriffsform: Social Engineering

- **Identitätsdiebstahl – Mehrfaktor-Authentisierung umgangen**:

  „Ich kann keine Text-Nachrichten empfangen, während ich telefoniere.“

- **Mensch wird zur Kooperation überzeugt**

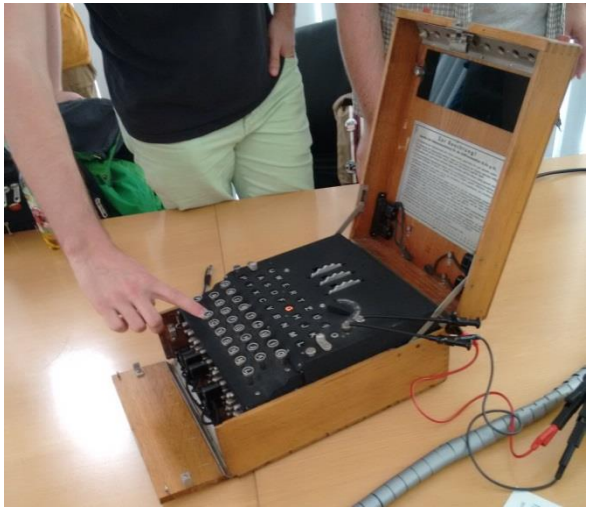
  Stress, Hilfsbereitschaft, Erpressung, Rhetorik

  (Ethos, Pathos, Logos) …

- **Abwehr: Schwierig**
  - Widerstandsfähige Software
  - Schulung der Mitarbeiter
  - Härtung der Geschäftsprozesse

5. Zusammenfassung

1. Mehrfaktor-Authentisierung:
   - Wesentlicher Sicherheitsgewinn
   - Teil des BSI-Grundschutz Katalogs
2. WebAuthn
   - Offener Standard für Web-Apps, Fokus: End-Nutzer
   - Schutz vor Phishing
   - Stand: Candidate Recommendation
3. Sicherheit
   - Mehrfaktor-Authentisierung ist ein Teil
   - Angriffe z.B. via Social Engineering möglich
   - Abwehr im Geschäftsprozesse



Abschluss

Vielen Dank für Ihre Aufmerksamkeit!

Wir freuen uns Sie an unserem Stand begrüßen zu können:

Stand: 12 Ebene 1

(neben der Information an den Rolltreppen)