Fingerabdruck-Authentifizierung

Die dunkle Seite des daktyloskopischen Identitätsnachweises

twitter.com/ja_sie | jasie.de/fingerprint

Überblick

I. Ausflug: Authentisierung, Authentifizierung, Autorisierung

II. Fingerabdruck-Authentisierung & -Authentifizierung

III. Gefahren bei FA-Identifikationsnachweis

IV. Datenschutzrecht biometrischer Daten

Fun Facts

- *Daktylos* altgr. Finger
- wahrscheinlich einzigartig
- nur Menschen, Affen, Koalas
- Adermatoglyphie: keine Papillarleisten
- erster Mord mit FA aufgeklärt: 1892 in Argentinien

I. Authentisierung, Authentifizierung Autorisierung

I. AAA: Authentisierung

1. **Authentisierung**:

Nachweis einer Person

z.B. Eingabe von Login-Daten in einem EDV-System

I. AAA: Authentifizierung

1. **Authentisierung**:

Nachweis einer Person

2. **Authentifizierung**:

Prüfung der behaupteten Authentisierung

z.B. durch das EDV-Systems inkl. Ergebnis

I. AAA: Autorisierierung

1. **Authentisierung**:

Eingabe von Login-Daten in einem EDV-System

2. **Authentifizierung**:

Prüfung der behaupteten Authentisierung

3. **Autorisierung**:

Prüfung der Rechte + Gewährung/Verweigerung

z.B. Adminrechte einräumen

II. Fingerabdruck-Authentisierung & -Authentifizierung

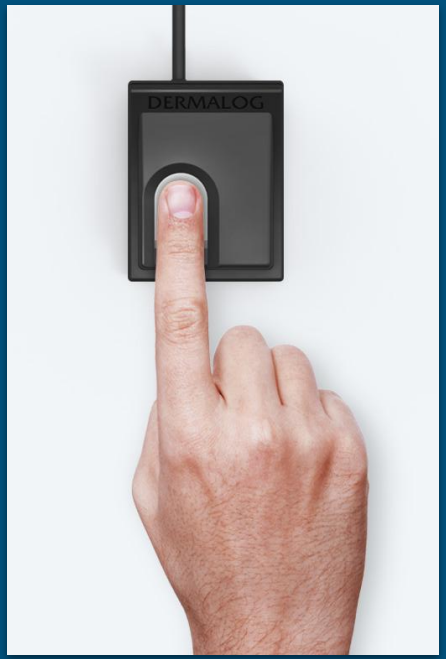
2) FA-Auth: Scanner - h.a.

- **halbautomatische Scanner**
  → schmale Fläche, Finger drüberziehen
  meist kapazitiver Sensor

2) FA-Auth: Scanner - v.a.

- halbautomatische Scanner
  → schmale Fläche, Finger drüberziehen
  meist kapazitiver Sensor

- **vollautomatische Scanner**
  → ganzer Abdruck auf einmal erfasst
  oft optischer Sensor

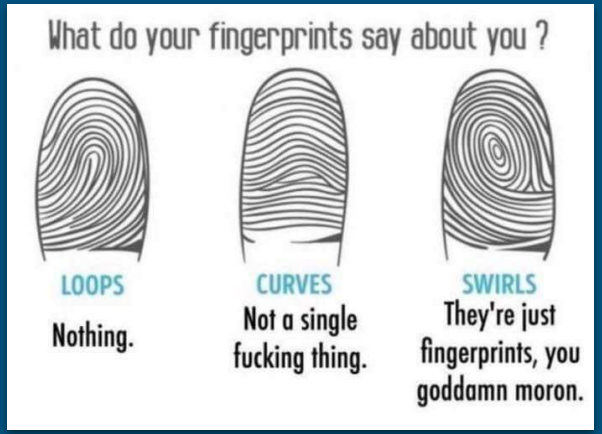


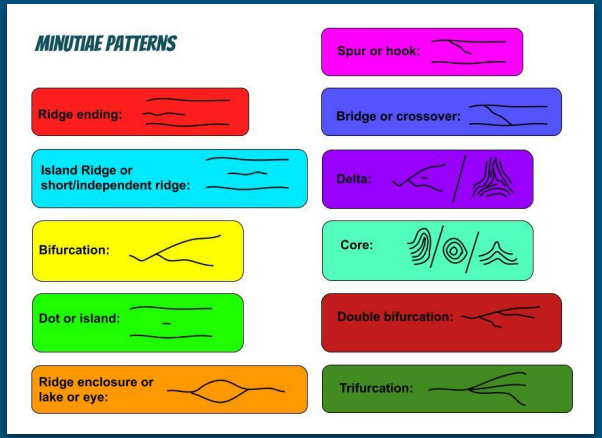
2) FA-Auth: Scannen

- **optisch**: Helligkeitsunterschiede, via CDD leichter zu täuschen
- **kapazitiv**: elektrische Ladungsunterschiede, via Kondensatorzellen
- Abbild der Papillarlinien des Fingers → “Daktylogramm”

2) FA-Auth: Speichern

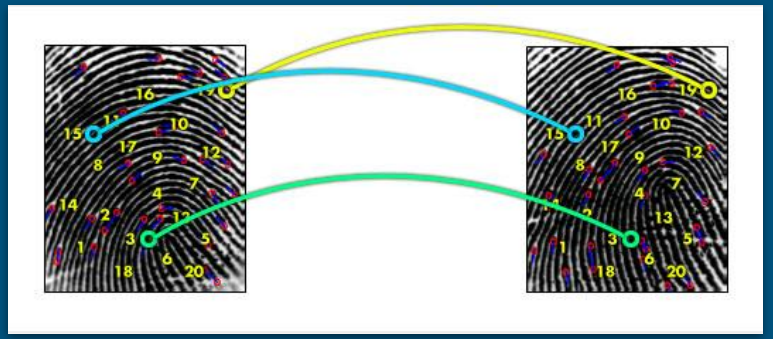
- *Ridges* oder *Minuzien*
- meist Speicherung als Hash-Code
  → FA aus Daten nicht mehr rekonstruierbar
- oft nur Teilabdruck gespeichert





2) FA-Auth: Abgleichen

- **Korrelationsverfahren**
  Pixelvergleich auf Bildern
- **Graterkennungsverfahren**
  Vergleich von ‘Ridges’ & ‘Valleys’
- **Minuzienbasierte Verfahren**
  Vergleich von ~40 gehashten Minuzien



- Probleme: Rotation, Position, Verzerrung, Veränderungen, Grad der Übereinstimmung

III. Gefahren des daktyloskopischen Identitätsnachweises

III. Gefahr 1: Ungenauigkeit

- Roger Grimes company: 700 Mitarbeiter & mehrere “gleiche” FA
- Paper 2017: 2 von 3 Handys mit Universal-Fingerabdruck entsperrt
- Fingerabdruck-Scanner mangelhaft

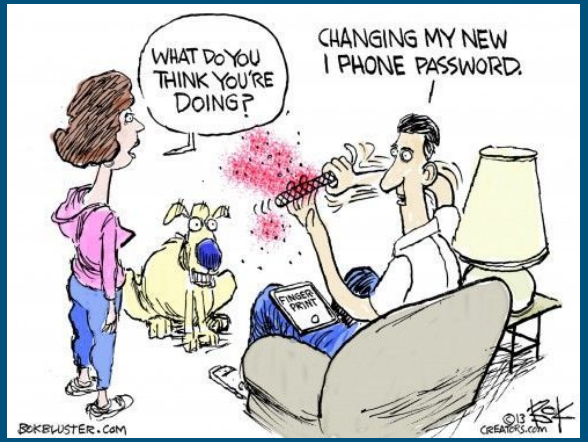
III) Gefahr 2: FA leicht stehlbar

- physisch stehlbar: Fingerabdruck überall verteilt
  - CCC 2008 FA eines Politikers von Glas
  - CCC 2013 Fake-Finger aus Latex
  - Knetmasse, Alleskleber…

- digital stehlbar: beim Scan
  - Black Hat Convention 2015 Fake-App mit FA-Scan
  - Hack des Abdruckscanners oder des Storage

III) Gefahr 3: FA nicht änderbar

- einmal in fremden Händen: für immer kompromittiert
- Passwort jederzeit änderbar
- Passwort je Auth variabel
- 2015 Hack: FA von 5.6 Mio US-Amis



III) Gefahr 4: FA nicht geheimhaltbar

Fingerabdrücke physisch und keine „Zeugenaussage“

→ 5. Zusatzartikel des Auskunftsverweigerungsrechts gilt nicht

→ Polizei darf ohne deine Zustimmung dein Gerät mit biometrischen Daten entsperren

“ich hab nichts zu verbergen”

IV) Biometrie im Datenschutzrecht

IV) Datenschutzrecht bei biom. Daten

- Pflicht der Speicherung von FA in BRD
  → im Reisepass seit 2017
  → im Personalausweis seit August 2021

- Fingerabdrücke = *biometrische Daten nach Artikel 9 Abs. 1 DSGVO und*
  = besondere Kategorien personenbezogener Daten im Sinne von § 26 Abs. 3 BDSG
- Verarbeitung von biometrischen Daten *nach Artikel 9 Abs. 1 DSGVO grundsätzlich verboten*

IV) Schutz deiner biom. Daten

- kontaktlos auslesbar (NFC)
- NFC-Schutzhüllen
- ausprobieren mit NFC-Reader App

Fazit

- FA nicht sicherer als Passwort
- Fingerabdruckpreisgabe erzwungen trotz DSGVO
- Fingerabdruck in Kombi mit Passwort akzeptabel

Quellen

- *3 Gründe, niemals Fingerabdruck-Sperren auf Mobiltelefonen zu verwenden* | Mark Yates, 12. Juli 2016
  https://www.avg.com/de/signal/3-reasons-to-never-use-fingerprint-locks
- *Fingerabdrucksensor: So funktioniert der biometrische Scan* | Julian Schulze, 2018
  https://blog.deinhandy.de/fingerabdrucksensor-so-funktioniert-der-biometrische-scan
- *6 reasons biometrics are bad authenticators* | Roger A. Grimes, 4. Januar 2019
  https://www.csoonline.com/article/3330695/6-reasons-biometrics-are-bad-authenticators-and-1-acceptable-use.html
- *Authentisierung, Authentifizierung und Autorisierung* | Agnieszka Czernik, 24. Juni 2016
  https://www.dr-datenschutz.de/authentisierung-authentifizierung-und-autorisierung/
- *#PersoOhneFinger* | digitalcourage, 2. Februar 2021
  https://digitalcourage.de/blog/2021/personalausweis-ohne-fingerabdruecke
- *Fingerabdrucksysteme* | Prof. J. Köbler & Matthias Schwan, 12. Dezember 2004
  https://www2.informatik.hu-berlin.de/Forschung_Lehre/algorithmenII/Lehre/SS2004/Biometrie/04Fingerprint/html/fingerabdrucksysteme.html