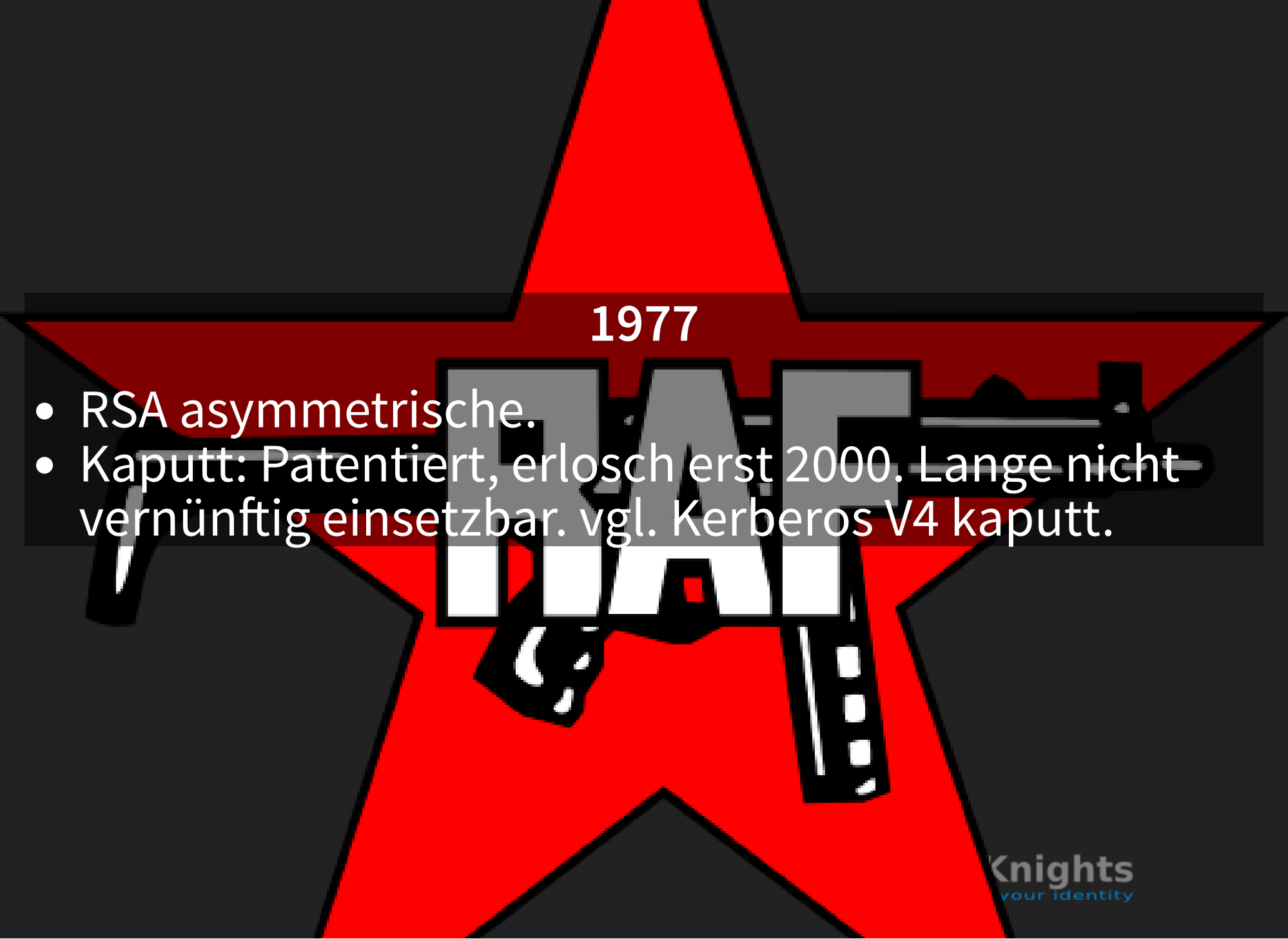
Cornelius Kölbel

- Cornelius Kölbel
- 1973: *
- 1998: Beruflich in IT
- 2004: 2FA

NetKnights
securing your identity

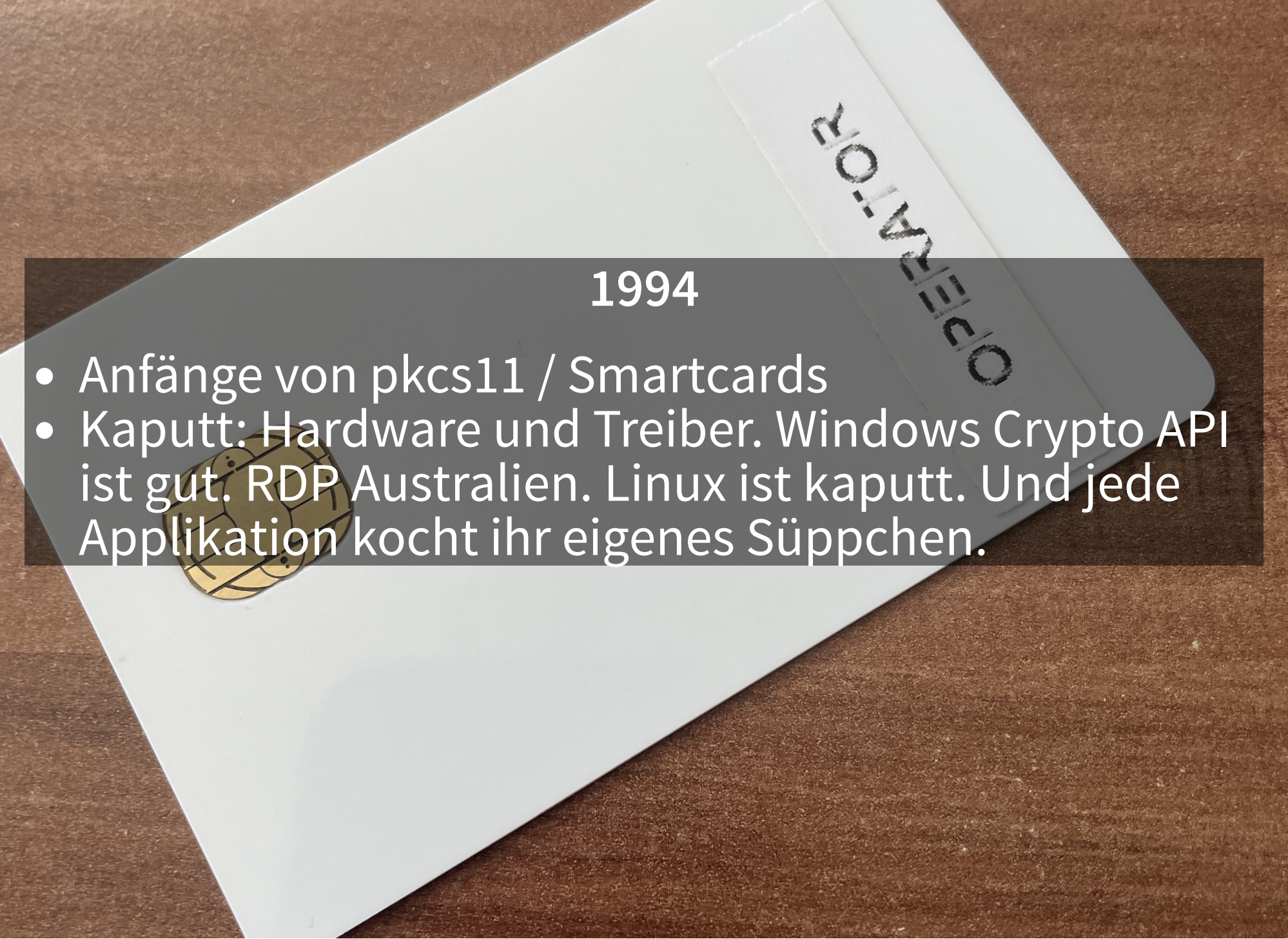


1977

- RSA asymmetrische.
- Kaputt: Patentiert, erlosch erst 2000. Lange nicht vernünftig einsetzbar. vgl. Kerberos V4 kaputt.

1980er

- RSA SecurID. symmetrischer Schlüssel
- Mangels Hardware?
- Kaputt: Proprietär. Hardware-Token hören irgendwann willkürlich auf, zu funktionieren. (901099) John the Ripper.



1994

- Anfänge von pkcs11 / Smartcards
- Kaputt: Hardware und Treiber. Windows Crypto API ist gut. RDP Australien. Linux ist kaputt. Und jede Applikation kocht ihr eigenes Süppchen.

1999

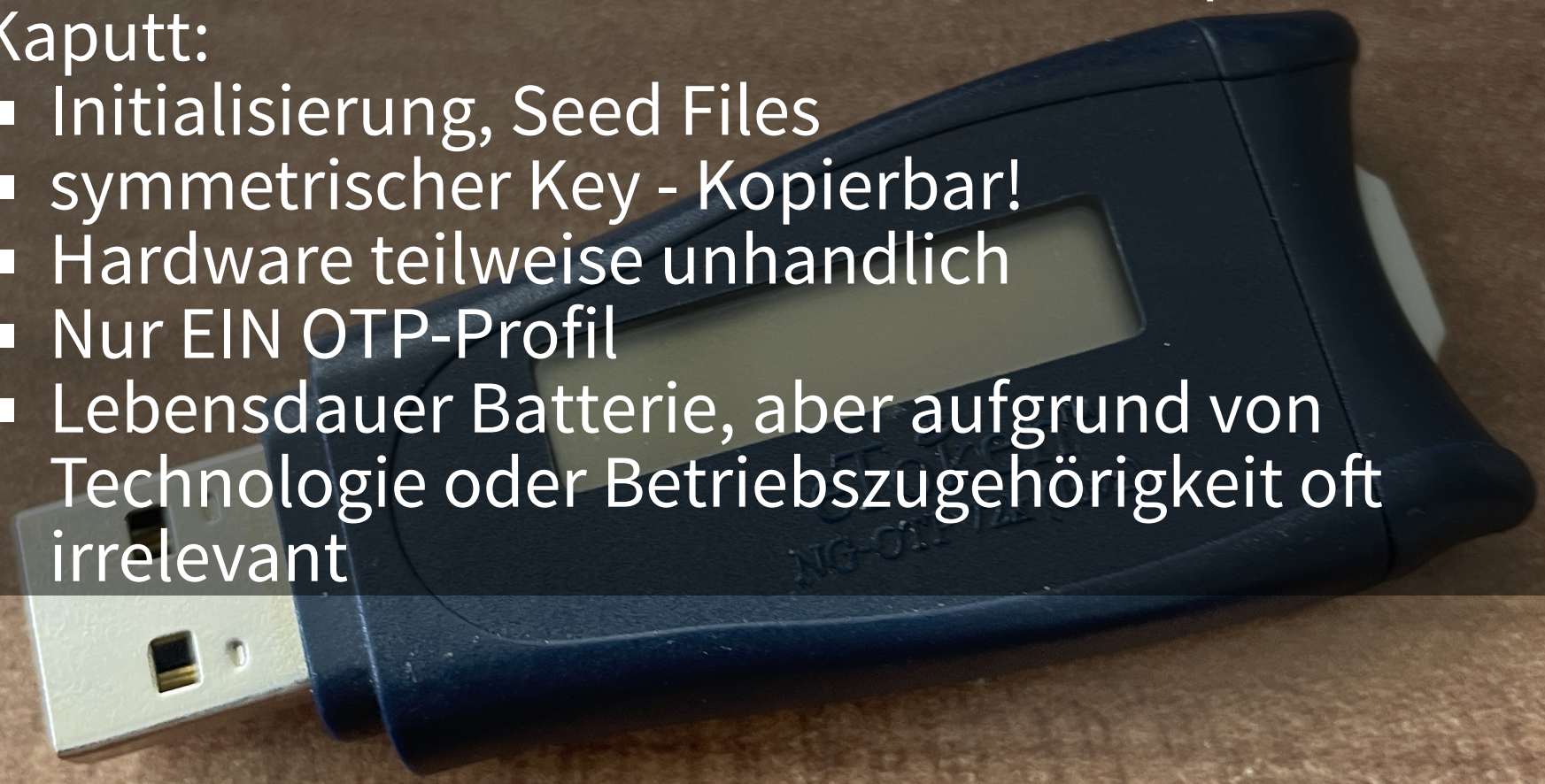
- X.509 Zertifikate und CRLs. (PKI)
- Kaputt:
  - Komplex. Großer Beratungsaufwand
  - x509 Zertifikate laufen aus (Gültigkeit)
  - Keine Aktuellen CRLs. Ungültige Zertifikate können nicht gefunden werden.
  - Problem noch heute: vgl. Gültigkeit von Webserver-Zertifikaten.

2003

- MOTP: https://motp.sourceforge.net/
- Feature Phones!, MD5, 10-Sekunden-Fenster
- Alternative zu RSA SecurID
- Smartphones und OATH nicht existent
- Kaputt: Abhängig von einem Typus Hardware. Feature-Phones nicht mehr existent.

2004: Initiative for Open Authentication (OATH)

- OATH: HOTP, TOTP, OCRA
- Hardware, die 2005 HOTP macht (!TOTP)
- Offener als RSA SecurID, initialisierbar, preiswert
- Kaputt:
  - Initialisierung, Seed Files
  - symmetrischer Key - Kopierbar!
  - Hardware teilweise unhandlich
  - Nur EIN OTP-Profil
  - Lebensdauer Batterie, aber aufgrund von Technologie oder Betriebszugehörigkeit oft irrelevant



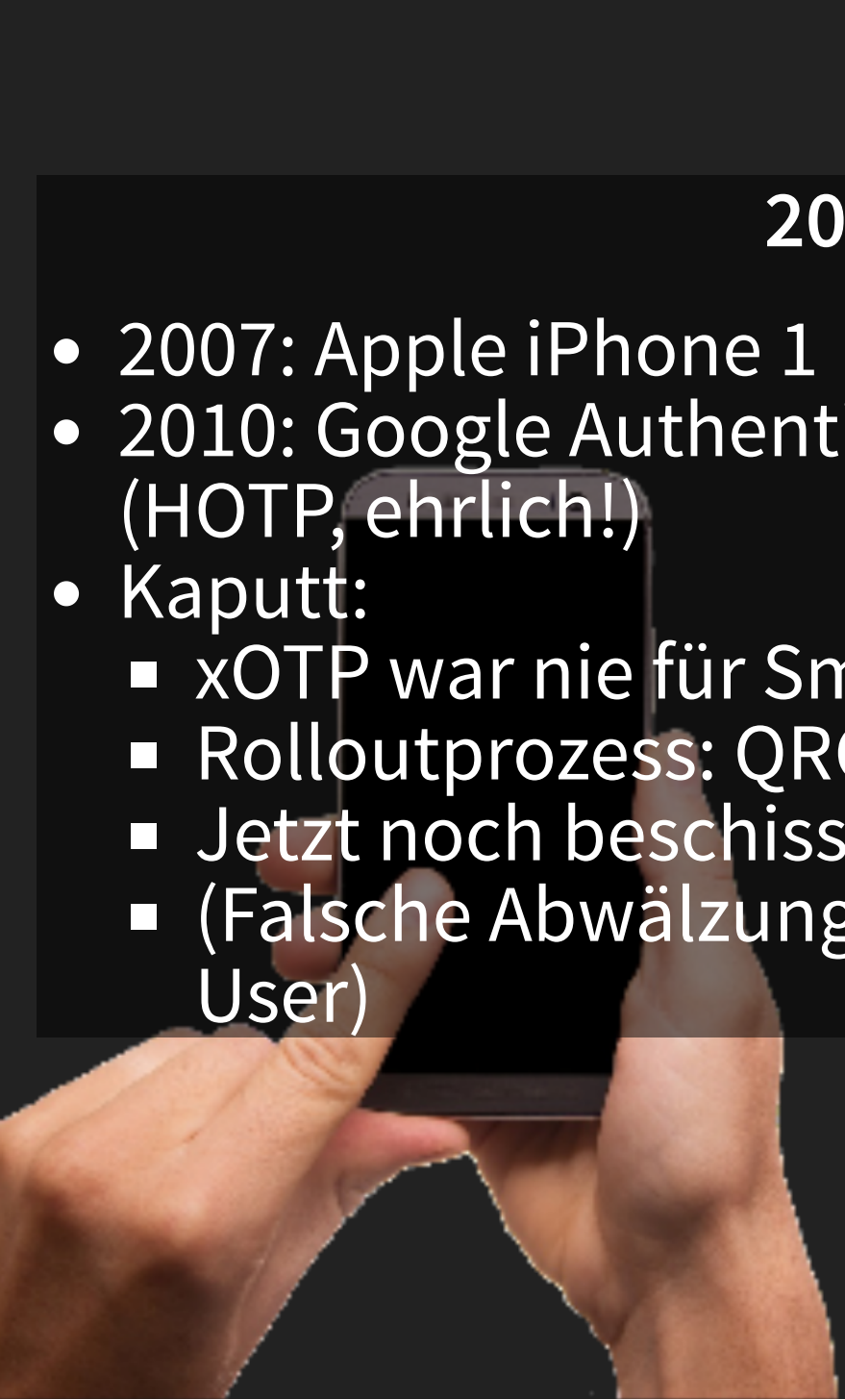
2008: Yubikey

- OTP AES und OTP HOTP
- keine Batterie,funktioniert ewig, blinde Benutzer! https://www.yubico.com/why-yubico/yubico-innovation-history/
- Kaputt:
  - Teuer: OTP-Only damals 25€
  - Benötigt USB (ok, NFC)
  - Kann nur einen (zwei) OTP Profile speichern.

NetKnights
securing your identity

2007 / 2010

- 2007: Apple iPhone 1
- 2010: Google Authenticator, Adaption RFC4226 (HOTP, ehrlich!)
- Kaputt:
  - xOTP war nie für Smartphone gedacht
  - Rolloutprozess: QRCode angreifbar
  - Jetzt noch beschissener - weil Backup
  - (Falsche Abwälzung der Verantwotung auf den User)



NetKnights
securing your identity

2013 / 2016

- 2013: FIDO, U2F, UAF
- 2016: Arbeiten an FIDO2 (WebAuthn/CTAP)
- Kaputt:
  - Schleppende Verbreitung: Paypal - Scheiße: 1 x FIDO2, 1 x SMS
  - Design für Cloud-Dienste - nicht für Enterprise
  - Nutzer kann Registrierung nicht nachvollziehen
  - Unternehmen kann nicht tracken, wo ein Mitarbeiter seinen Token registriert hat.
  - Die Unmöglichkeit der Verwaltung wird auf den User abgewälzt.

Conclusio

- Nicht alleine Krypto bestimmt die Qualität eines zweiten Faktors
- Sondern: Benutzbarkeit, Verbreitung, Verwaltbarkeit
- Smartphone-Apps, FIDO2: Verantwortung wird auf den User abgewälzt

Successful authentication is a matter of smooth workflows


NetKnights
securing your identity