RSA

OWN YOUR IDENTITY.

OTP ist tot!
… lang lebe OTP?!?

Ingo Schubert

Global Cloud Identity Architect

RSA

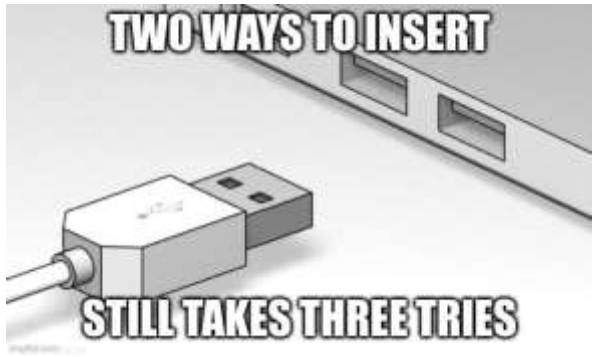
Die 90er

- OTPs waren lange Zeit fast alternativlos für starke Authentifizierung
  - … von X.509 Zertifikaten in homöopathischen Dosen mal abgesehen.

- OTPs zwar nicht perfekt aber
  - Relativ hohe Sicherheit
  - Akzeptables Benutzererlebnis
  - Praktikabel

Nachteile von OTP

- Nutzerfreundlichkeit
  - Ähnlich wie USB-A Stecker: manchmal klappt es nicht auf Anhieb.
  - Ablesen, vertippen, ablesen, eintippen… Erfolg!



- Hardware OTPs
  - Warum einen Hardware Token wenn das Smartphone immer dabei ist?

- Eingeschränkte Phishing Resistenz
  - Time-based OTP gegen „offline“ Phishing
  - FIDO2 bietet besseren Schutz gegen Phishing

Vorteile von OTP

- Funktioniert von überall
  - Keine Netzwerkverbindung des Authentifikators (Token) notwendig
  - Keine USB, NFC, Bluetooth oder sonstige Schittstelle notwendig

- ~~Legacy~~ Legendary-Applikationen und Systeme
  - Werden uns noch eine ganze Weile begleiten
  - OTPs oft die einzige Möglichkeit für starke Authentifizierung

- MFA Fatigue / Push bombing
  - Netter Versuch!
  - … und jetzt wieder: ablesen, vertippen, ablesen, eintippen… Erfolg!

- Hardware OTPs
  - Objektiv sicherer als softwarebasierte OTPs (und Push) in den meisten Fällen
  - Kein Smartphone notwendig

Es ist noch zu früh…

- … OTPs als Authentifizierungsmethode zu ignorieren.
- Als alleinige Methode (one size fits all) ist OTP nicht mehr sexy genug.
- Als eine der möglichen Methoden einer modernen MFA Lösung hat OTP aber seinen berechtigten Platz da OTP…
  - … offline funktioniert,
  - eine breite Auswahl an Formfaktoren und bietet (Sicherheits-Niveaus, unabhängig von Software/Hardware) und
  - universell einsetzbar ist (Legacy Anwendungen).

Ist ja klar, daß RSA das behauptet!

- RSA SecurID unterstützt noch viel mehr Methoden u.a.
  - FIDO2
  - Biometrie
  - Push
  - QR Code
  - …
- Der Einsatz von OTP im Allgemeinen und Hardware-OTP im Speziellen nimmt ab
- HW OTP hat seine Daseinsberechtigung
  - Unabhängig von anderer Hardware und Software (BYOD)
  - Sicherheitsniveau

Es kommt nur teilweise auf den Formfaktor an!

Egal ob HW oder SW, OTP oder irgendeine andere Methode:
Es fängt alles bei der Registrierung an!

- Viel wichtiger als der Formfaktor selbst ist wieviel Vertrauen während der Registrierung „aufgebaut“ wird
  - Später kann nicht mehr Vertrauen in den Authentifikator gelegt werden als am Anfang aufgebaut wurde.

- Nicht jede Methode ist gleichwertig.
  - Einordnen der verschiedenen Methoden in Vertrauensstufen

Hybrid OTP/FIDO2 Token: RSA DS100

- Der DS100 ist ein kombinierter FIDO2 und OTP Token
  - Mit eigenem Display
  - USB-C
  - Laufzeit bis zu 9 Jahre

- Taste hat zwei Funktionen
  - FIDO2 Bestätigung
  - OTP „eintippen“ (simuliert ein Keyboard)

- „DS“ = „Distributed Seeding“
  - Tokens werden von den Benutzer*innen selbst registriert

OWN YOUR
IDENTITY.