TEMET
end-to-end IT security

Nach Paperless kommt nun Passwordless

Daniel Brunner

21.05.2019

Über den Referenten

Daniel Brunner

- ★ Informatiker EFZ
- ★ Certified Scrum Product Owner

Security Consultant

- ★ In der IT Security tätig seit 2011

Spezialgebiete

- ★ Sicherheitsanalysen
- ★ Agiles Projektmanagement
- ★ Risk Management

Kontakt

- ★ Mobile: +41 79 452 18 75
- ★ E-Mail: daniel.brunner@temet.ch

Geschichte

TEMET
end-to-end IT security

Idee

★ BC	753	Kennwort beim römischen Militär
		Challenge-Response-Authentifizierung

Umsetzung

★ AD	1961	Passwort beim Compatible Time-Sharing System
★	1974	Passwort als Hash in der 6th Edition von Unix

Erweiterte Sicherheit

★	1984	Method and apparatus for positively identifying an individual (RSA SecurID Patent: US4720860A)
★	2005	HOTP: An HMAC-Based One-Time Password Algorithm (RFC 4226)
★	2011	TOTP: Time-Based One-Time Password Algorithm (RFC 6238)

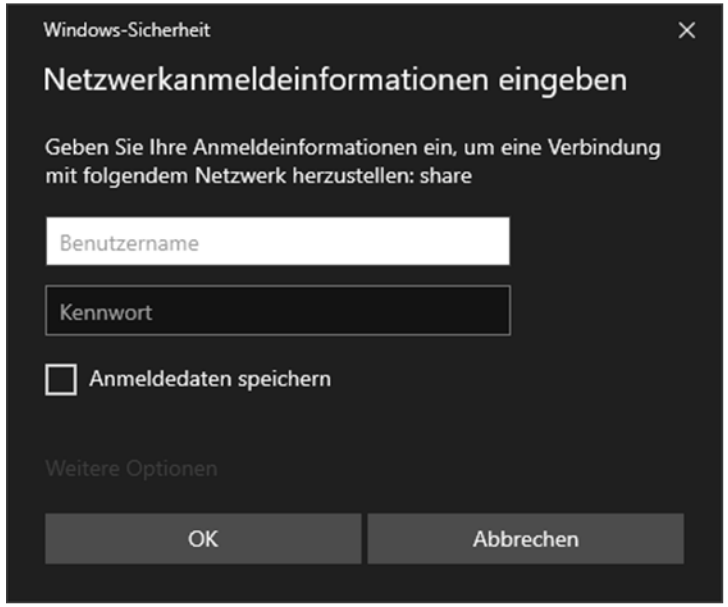
…

★	2013+	Gründung FIDO Alliance

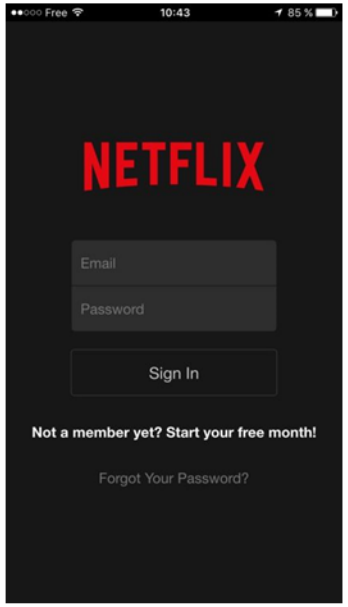
Wo melden wir uns an?

TEMET
end-to-end IT security

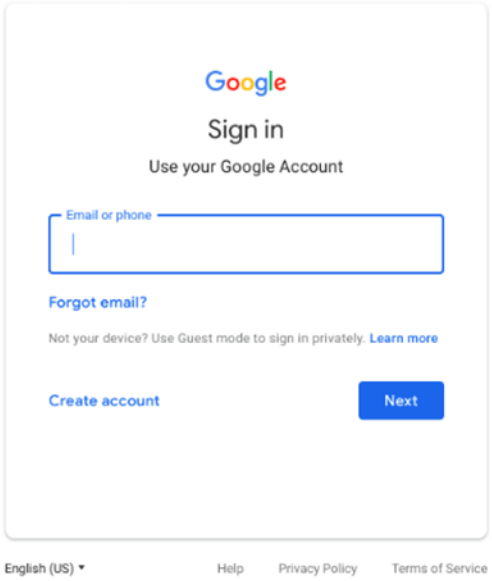
Betriebssystem



Mobile App



WWW



Login! Gerne, aber wie denn?

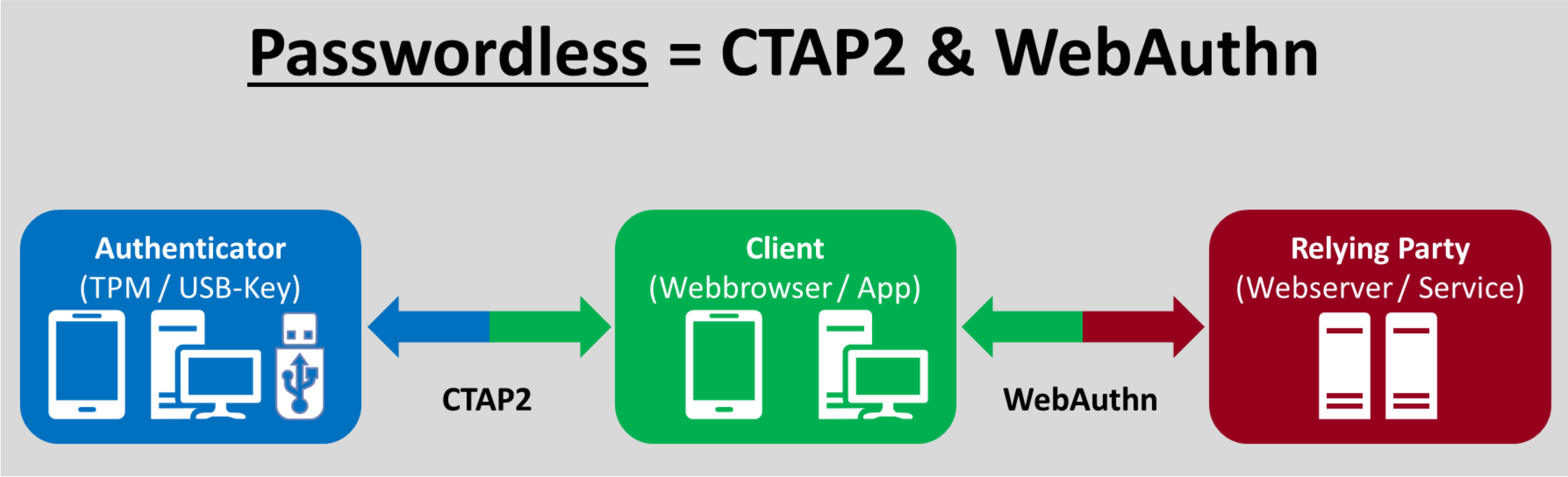
TEMET
end-to-end IT security

FIDO Alliance

- ⋆ Client to Authenticator Protocols (CTAP2)

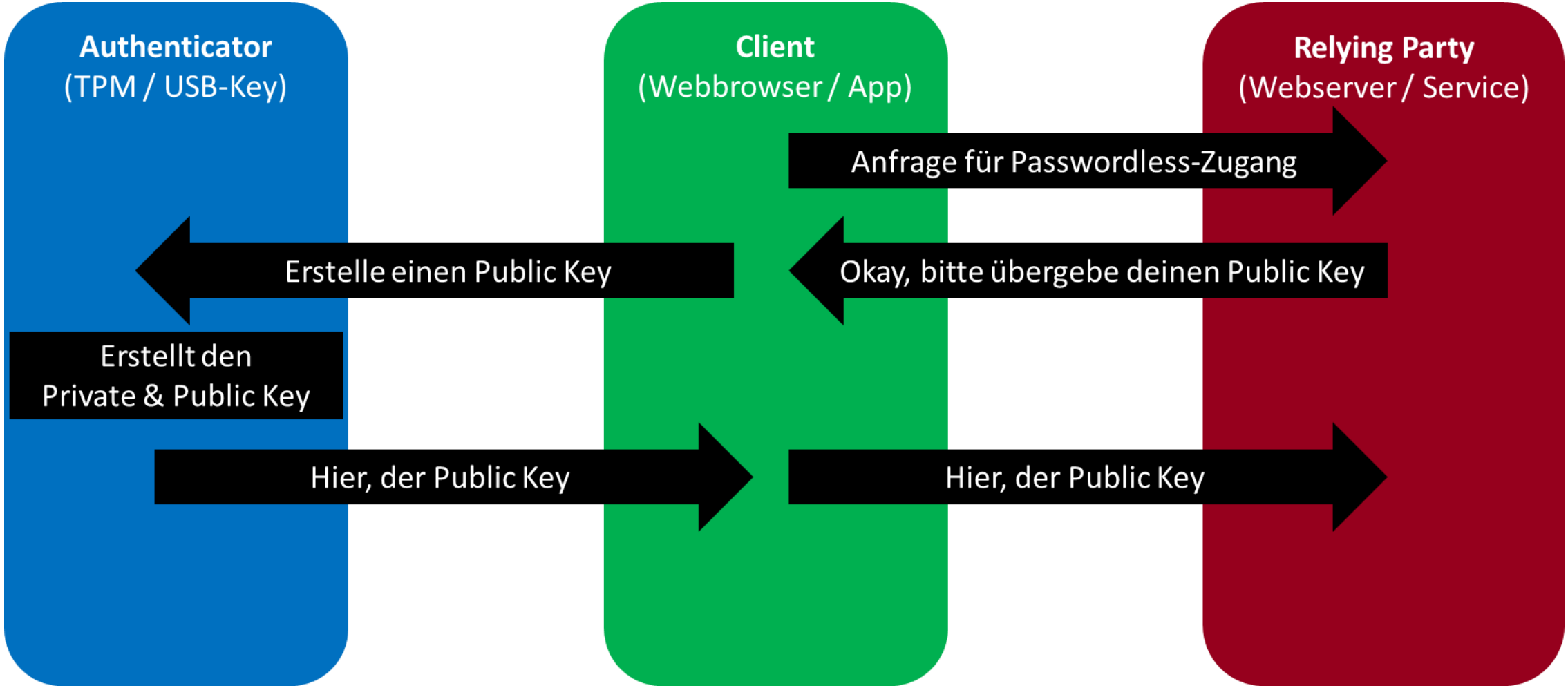
W3C

- ⋆ Web Authentication (WebAuthn) Standard



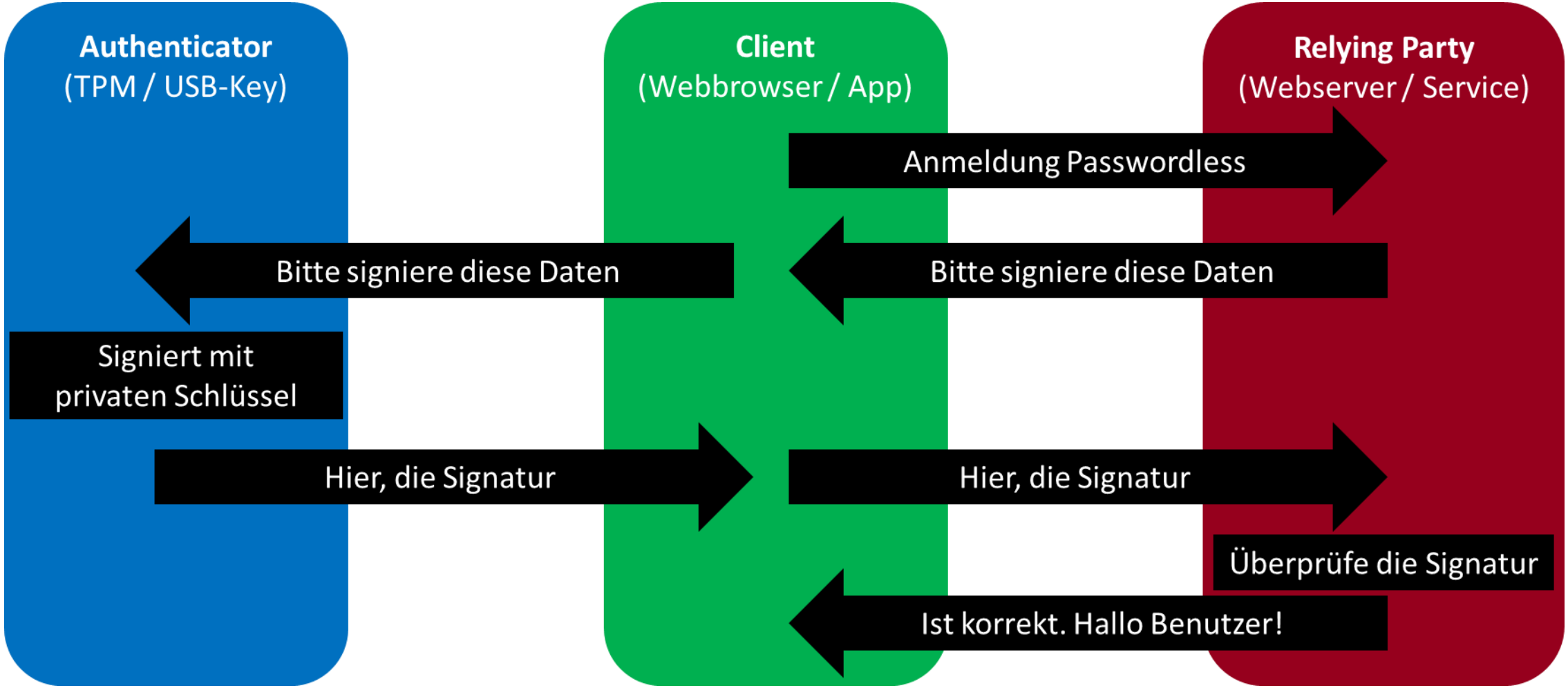
Wie funktionieren die Protokolle?

Registration



Wie funktionieren die Protokolle?

Authentifizierung



Gibt es nur Passwordless?

TEMET
end-to-end IT security

W3C

★ Web Authentication (**WebAuthn**)

FIDO Alliance

★ FIDO Universal Authentication Framework (FIDO UAF)

★ FIDO Universal Second Factor (FIDO U2F)

★ Client to Authenticator Protocols (**CTAP 1 & 2**)

FIDO2 Standard

★ WebAuthn & CTAP1 → Zweiter Faktor

★ WebAuthn & **CTAP2** → Passwordless

Was ändert sich im Vergleich?

Die Handhabung und damit auch der sichere Umgang mit Passwordless Systemen.

- ★ Ist die Gefahrenlage gleich?
- ★ Weshalb haben wir nicht bereits Passwordless im Einsatz?
- ★ Was kommt nach Passwordless?

© Washington Post

Ist die Gefahrenlage gleich?

TEMET
end-to-end IT security

Passwort

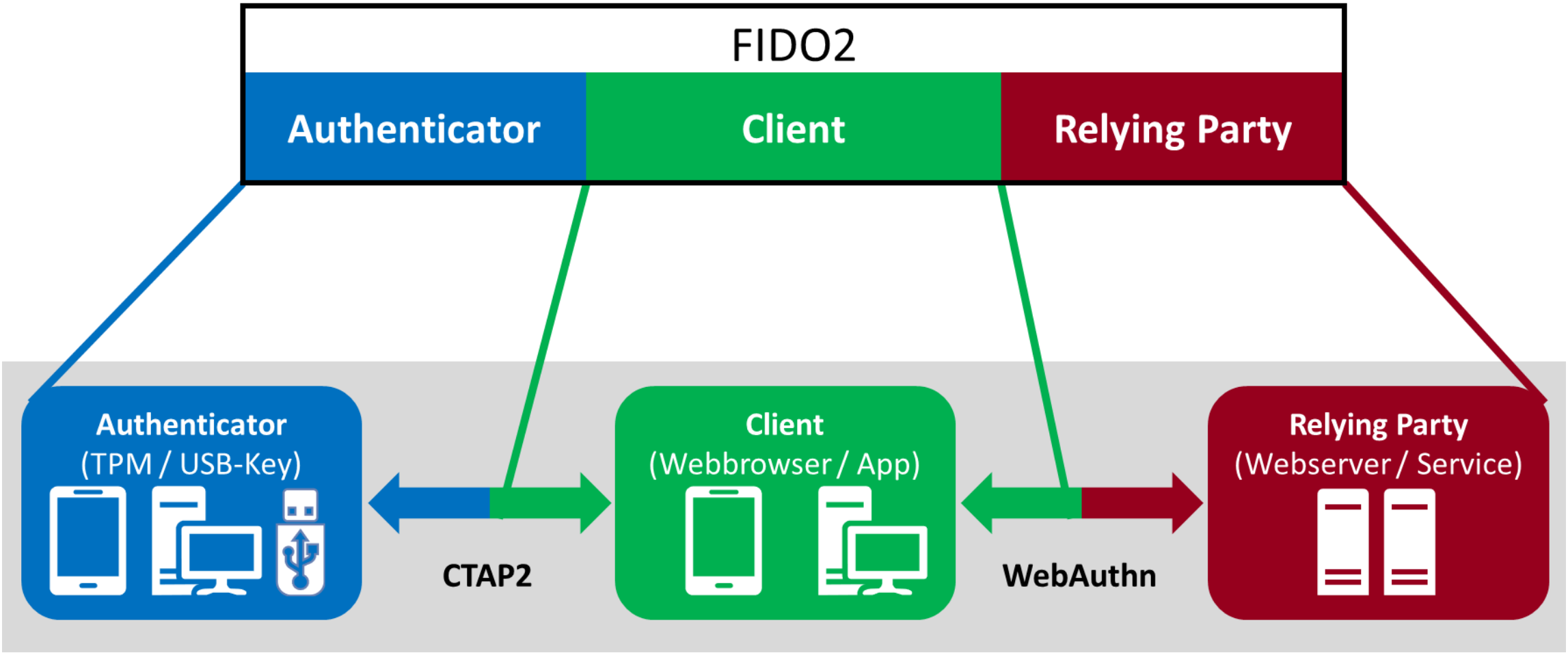
- ★ Shoulder-Surfing / CCTV
- ★ Auswertung der Anmeldeversuche
- ★ MiTM (SSL/TLS)
- ★ Malware
- ★ Phishing
- ★ Komplexere Passwörter erfordern ein noch besseres Gedächtnis oder Passwort Manager
- ★ Kollisionsberechnung des Hash (Passwort)
  - 2.3 Milliarden SHA256 Berechnungen pro Sekunde mit einer Nvidia Titan X

Passwordless

- ★ Diebstahl / Verloren
- ★ Defekt
- ★ Notwendigkeit für step-up authentication
- ★ Reenrollment aufwändig für Endbenutzer
- ★ Komplexitätssteigerung und Abhängigkeit zu darunterliegenden Protokollen
  - Unsichere USB- oder Bluetoothprotokolle
  - Attacken auf die Firmware

Worauf warten wir?

Weshalb haben wir nicht bereits Passwordless im Einsatz?



Authenticator

Thetis BLE U2F Security Key

Apple T2 Chip

Google
Android 7

YubiKey 5 NFC

ASUS TPM-M R2.0

Apple iOS 11

Google Titan

Infineon SLB 9665TT2.0

Other FIDO2 Devices

Client

Chrome (Desktop)
- WebAuthn seit Mai 2018
- CTAP2 seit September 2018

Safari
- WebAuthn nicht unterstützt
- CTAP2 nicht unterstützt

Edge
- WebAuthn seit Oktober 2018
- CTAP2 seit Oktober 2018

Firefox
- WebAuthn seit Mai 2018
- CTAP2 seit Februar 2019

Windows Hello
- WebAuthn seit Oktober 2018
- CTAP2 seit Oktober 2018

Relying Party

TEMET
end-to-end IT security

JAVA Library
- WebAuthn seit ~ Q2 2018

Python Library
- WebAuthn seit ~ Q3 2018

PHP Library
- WebAuthn seit ~ Q3 2018

GO Library
- WebAuthn seit ~ Q1 2019

Und es werden mehr!

Was kommt nach Passwordless?

TEMET
end-to-end IT security

Passwordless wird nicht so schnell ersetzt, aber…

- ⋆ Machine Learning um Benutzerverhalten zu analysieren → Loginless
  - Bekanntes Gerät (Fingerprint Browser / App)
  - Bekannte IPv4, IPv6 oder IPv6 Range (Privacy Extensions)
  - Benötigte Zeit für die Anmeldung

Was kommt nach Passwordless?

Passwordless wird nicht so schnell ersetzt, aber…

- ★ Multi-Device Signature «always-on» → Loginless
  - Geräteerkennung «nearby»
  - Signaturerstellung durch Metadaten:
    - ★ Batteriestatus des Gerätes
    - ★ Biometriedaten des Besitzers, wie etwa der Herzschlag

Schlusswort

- Es wissen nur wenige über die neuen Möglichkeiten bescheid.
- Wir werden gleich wie bei Paperless eine Koexistenz erleben.
- Sind Sie bereit, Ihr Passwort aufzugeben?

… zum Erfolg

Besten Dank
für Ihre Aufmerksamkeit!

TEMET AG
Basteiplatz 5
8001 Zürich
044 302 24 42
info@temet.ch
www.temet.ch