NEVIS

Hasta la vista Passwort-Authentisierung

Thomas Reisinger
IAM Technical Pre-Sales Consultant
Oktober 2019

NEVIS

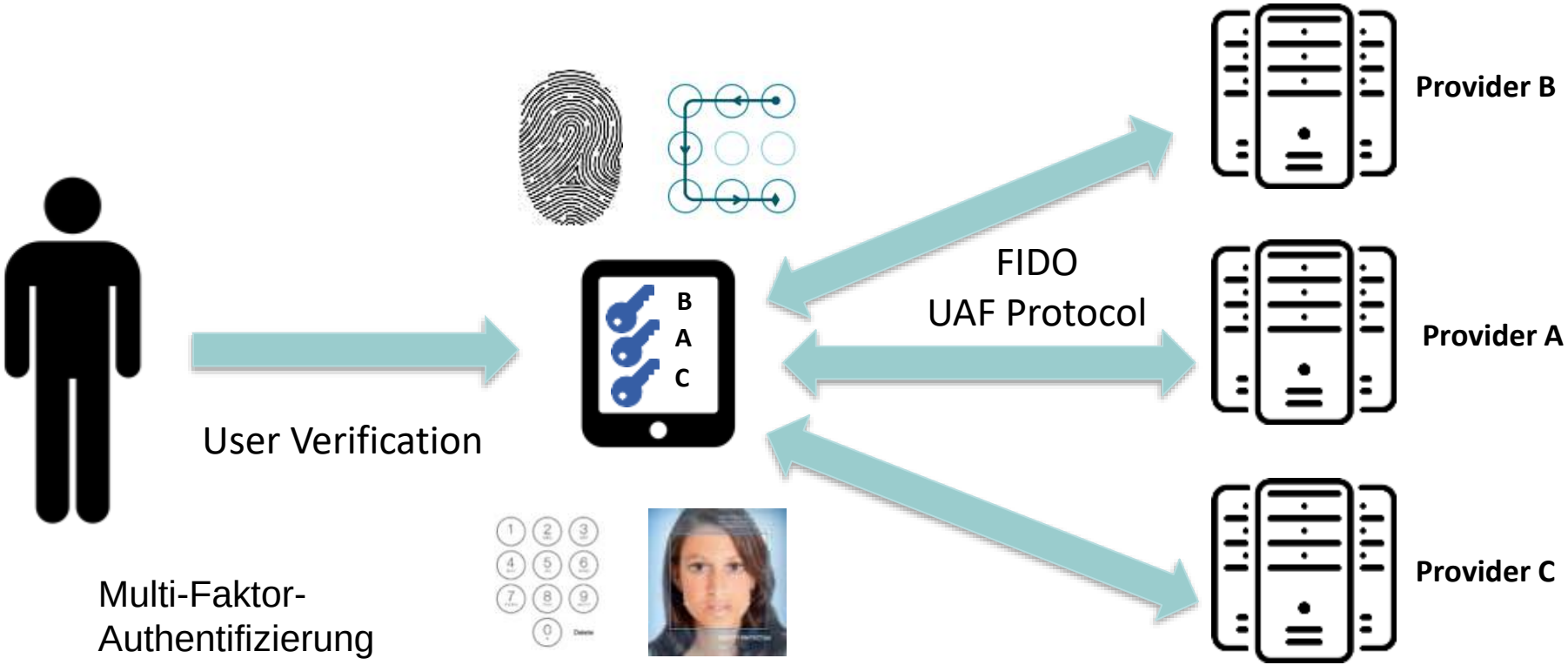
FIDO (Fast Identity Online)

UAF (Universal Authentication Framework)

passwortlose Authentifizierung

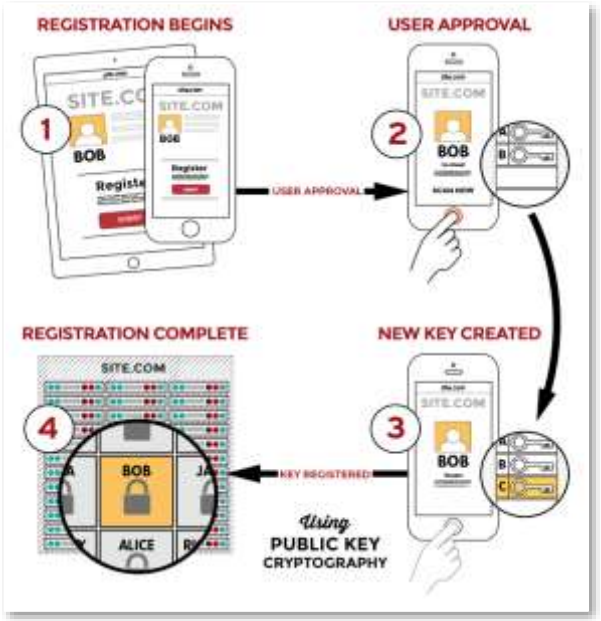
fido CERTIFIED UAF

Thinking in eco systems: Identity wallet



FIDO: How does it work?

Step 1: Registration



Step 2: Login / TRX Confirmation

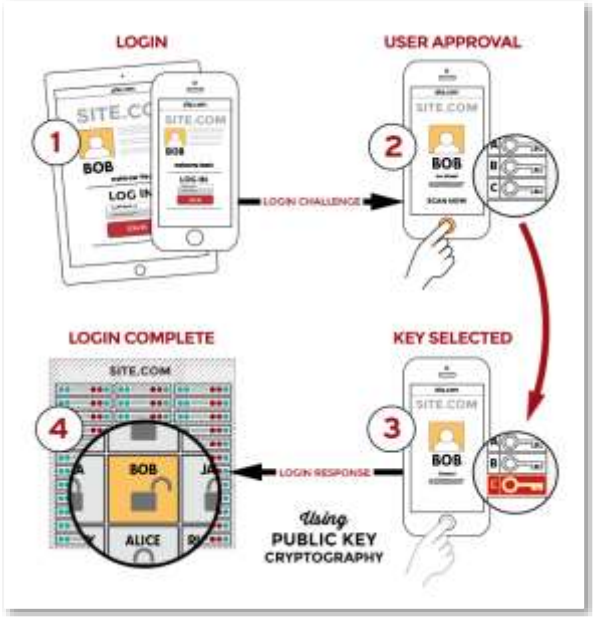
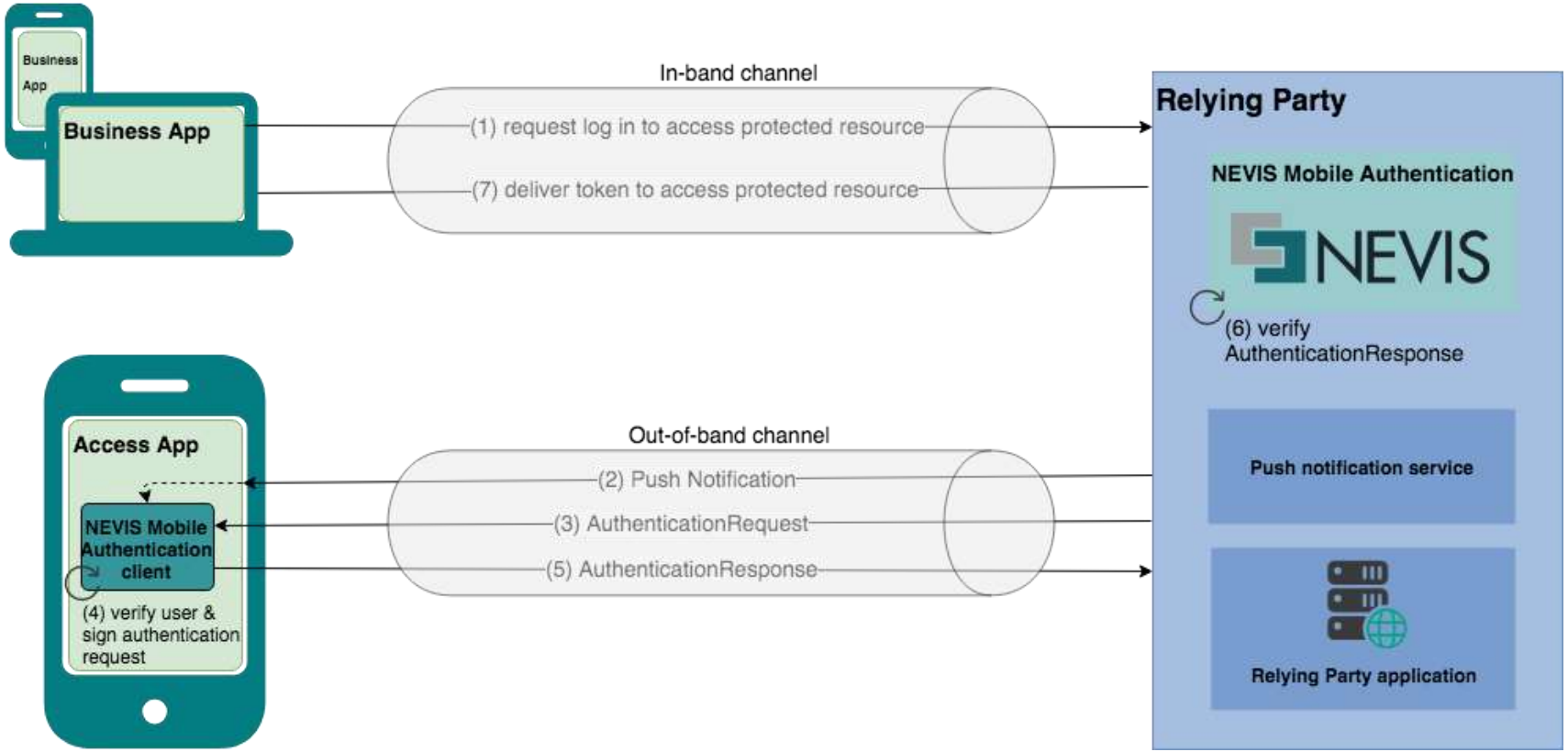


Image Source: https://fidoalliance.org/specifications/overview/

Out-of-Band Authentication – Multiple Devices



Why choose NEVIS Mobile Authentication?

Highlights:

- Easy and user friendly
- Highly secure and high standards for privacy
- Complying with strict authentication regulations (PSD2, NIST and HIPAA)
- Based on FIDO Standard
- Certified by FIDO Alliance

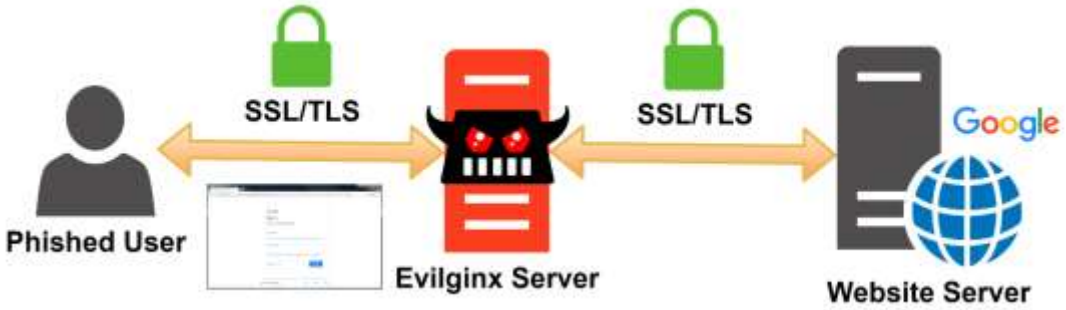
NEVIS

Phishing 2.0 Beispiel:

Evilginx 2 - Next Generation of Phishing 2FA Tokens

Evilginx2

- Developed by Kuba Gretzky Security Researcher/Poland
- Man-in-the-middle attack captures authentication tokens sent as cookies
- User credentials are also captured
- Lures clients with registered domain e.g. `faceboook.com`, `faceb00k.com` or special characters (e.g. Cyrillic) homograph attacks
- Evilginx2 re-writes the complete Requests and Responses, client and target server doesn't recognize the "reverse-proxy"
- Bypasses many forms of 2FA



Demo Recording

source: https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/

How to mitigate such sophisticated attacks?

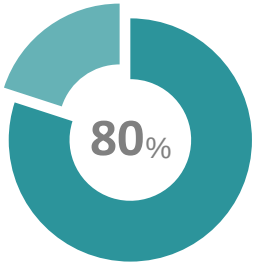
- Client authentication using Certificates – TLS mutual authentication
- Behavioral detection (nevisDetect)
- Client-Side obfuscated JavaScript with window.location, etc.
- Correlation between Session-Cookie and IP or other client specifics e- g. device recognition
- FIDO U2F (Universal 2 factor authentication)/FIDO2 (HW token required)

Fazit

- Periodic end user training and awareness for phishing/security is important
- Remember - 2FA is not a silver bullet against phishing!
- Multiple mitigation techniques are required to reduce the attack surface

Renowned customers count on NEVIS

NEVIS
protects



of Swiss
e-banking
transactions

Selected Customers

PostFinance DIE POST
UBS
Die Mobiliar Versicherungen & Vorsorge
GENERALI DEUTSCHLAND
swisscom
Helsana
helvetia
Julius Bär
SIX GROUP
QUILVEST
ZURICH
SFS
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
• DETEC • FDEA
• FDF • FDJP
SITEL
Ct. Fribourg
SIEN
Ct. Neuchâtel

NEVIS Customer Identity & Access Management
Facts & Figures


NEVIS


Danke! Fragen?