



# EAP-FIDO Proof of Concept

tnc23 Mobility Day | 09.06.2023

Jan-Frederik "Janfred"  
Rieckers



# Scope of the Proof-of-Concept

- ▶ Registration already done
  - In Practice this could be done by a web portal
    - Login via LDAP/SAML/OIDC/..., then register FIDO-Token
- ▶ Implementation wpa\_supplicant and hostapd
- ▶ Certificate check will check the Relying Party ID against certificate SANs.
  - Not yet implemented
- ▶ In the PoC-Code only one token per user is allowed
- ▶ No Discoverable Credentials/Residential Keys (Username-less login) yet.

# Protocol



# DFN



EAP-TLS (RFC5216, not the EAP-Method) Handshake

Inner Username

Relying Party ID, Additional Client Data,  
List of Key Identifiers

Request for Silent  
Authentication (CTAP2)

Signature

Signature

EAP-Success

## Details about Implementation

- ▶ [https://git.riekers.it/riekers/hostap/-/tree/eap\\_fido](https://git.riekers.it/riekers/hostap/-/tree/eap_fido)
- ▶ Relies on
  - Latest master of <https://github.com/Yubico/libfido2.git>
  - Latest master of <https://github.com/Intel/tinycbor.git>
- ▶ Current EAP-Type 57 (Not allocated, use with caution)
- ▶ PoC was created during tnc (Don't blame me for the code. I'm ashamed of it)

## Next steps

- ▶ Write specification with message format, ...
- ▶ Early allocation for EAP-Type codepoint from IANA
  - There is interest from relevant people at IETF, this should not be a problem
- ▶ FreeRADIUS implementation will be available soon after the spec is out (Thanks to Alan)
- ▶ Specification may be published as Informational RFC
  - Independent submission instead of going through EAP Method Update (emu) WG
  - People will (hopefully) still implement it

# Discussion/Questions?

DFN

## ► Contact

### ► Jan-Frederik Rieckers

Mail: [rieckers@dfn.de](mailto:rieckers@dfn.de)

Phone: 0049 30 884299-339

Fax: 0049 30 884299-370

Address:

DFN-Verein, Geschäftsstelle

Alexanderplatz1

10178 Berlin

