draft-janfred-eap-fido
A new EAP method based on FIDO keys

IETF 118 in Prague – HotRFC | 05.11.2023

Janfred Rieckers

Why do we need something new?

- Eduroam configuration is not trivial
  - It’s too easy to misconfigure eduroam
- Certificate check is hard. There is no implicit way to derive the expected certificate names, users need to configure it manually
- Bootstrapping problem especially in BYOD environment

What are the new requirements?

- Trivial configuration
  - Security properties must not depend on the ability of users to configure their security parameters correctly
  - Users have no idea what the parameters mean and what implications they have
- Don’t use passwords
  - Authentication by Knowledge with the requirement to reveal the knowledge is a bad idea.

How do we solve this?

- Use asymmetric crypto that is easy to provision:
  - FIDO keys \o/
  - Should be available on most new devices in Software.
  - Can also be used with hardware-token
- Provisioning via web frontend (currently out of scope for EAP-FIDO spec)
  - EAP server just needs access to the DB of known FIDO Public Keys
- TLS certificate parameters are implicit through realm configuration
  - Users do not need to configure anything security related.
  - We just use WebPKI, it’s used for WebAuthn during registration anyway.

What now?

- See the EAP-FIDO Draft (draft-janfred-eap-fido)
- We have a side-meeting on Monday (tomorrow) 18:00 in Karlin 4
  - We are looking for
    - Feedback on Design
    - Experience of EAP operators
    - Input from EAP/RADIUS server and/or supplicant implementers
    - Input from people with FIDO/WebAuthn/CTAP experience
- The work will also be presented in the emu WG session
- Or find me in the hallways.

- Contact
  - Jan-Frederik Rieckers

Mail: rieckers@dfn.de
Phone: 0049 30 884299-339
Fax: 0049 30 884299-370

Address:
DFN-Verein, Geschäftsstelle
Alexanderplatz1
10178 Berlin