DFN

DEUTSCHES FORSCHUNGSNETZ

Update on EAP-FIDO

(name change still comming. Sometime.)

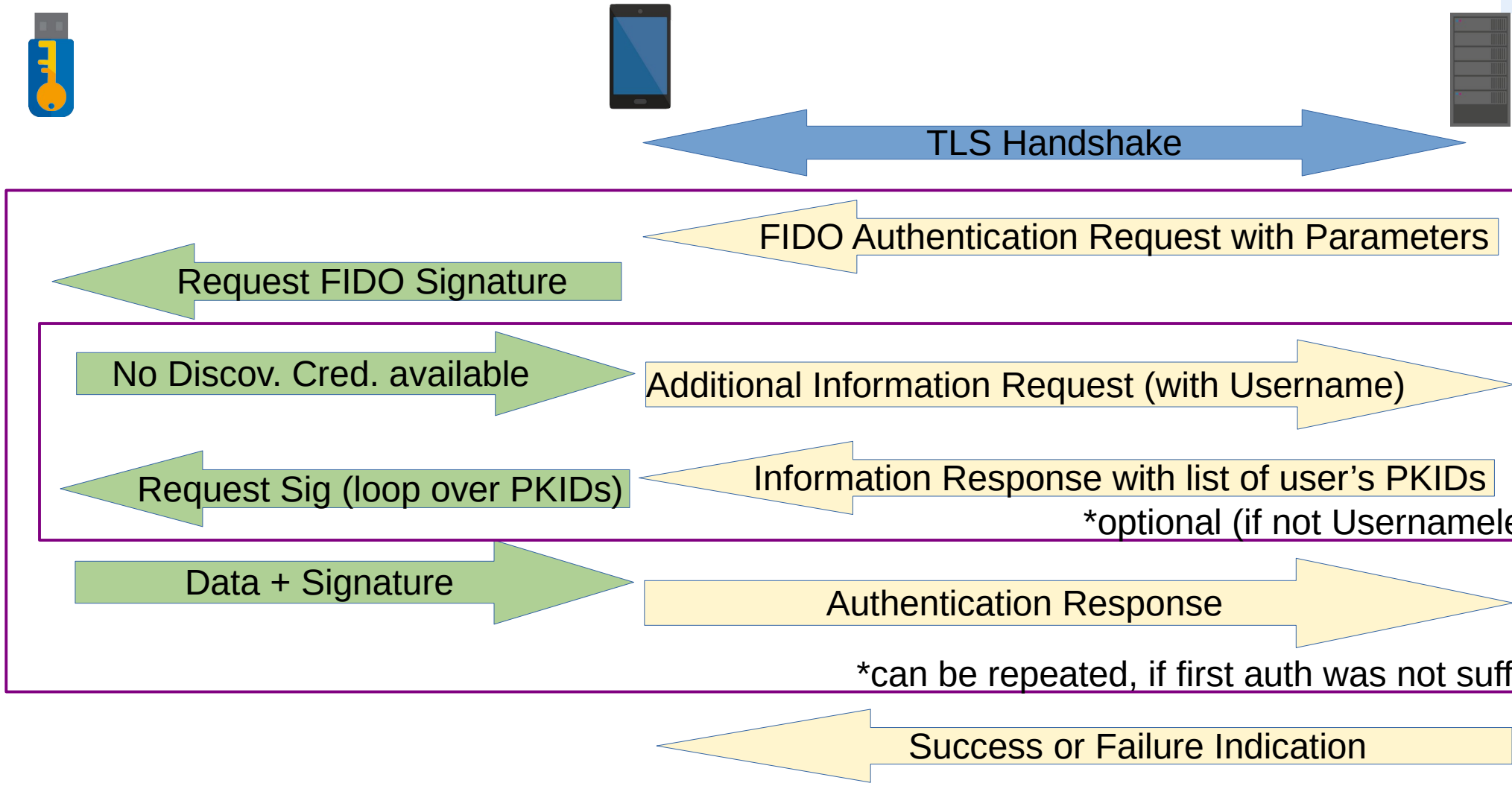
IETF 121 in Dublin – emu WG | 05.11.2024

Janfred Rieckers | DFN-Verein

Recap: Overview of the EAP-FIDO Protocol

- EAP-TLS based protocol with 2 phases
  - Phase 1: TLS Handshake
    - TLSv1.3
    - Server authenticates to the client through certificate
  - Phase 2: FIDO authentication
    - Server sends authentication parameters (up/uv required, …)
    - Supplicant requests signature from FIDO token through CTAPv2 or something similar
    - Supplicant sends signature back to the server
- Configuration: „One string to rule them all“
  - Aim to have only one string (ideally the institutions registered domain) that the user can be expected to know, everything else follows that.

Recap: EAP-FIDO Protocol Flow



Updates since IETF 120 (Vancouver)

- No new draft version, mainly due to work in the background
- New proof-of-concept implementation
- Discussion on the mailing list on FIDO challenges

Running code

- New Proof-of-Concept with additional features up and running (as of today!)
  - Registration of credentials via web portal
  - Possibility to set specific authentication requirements per credential (up/uv)
  - Re-Authentication if a silent authentication was performed, but up/uv was required for this specific credential
- Works in eduroam, tested here at IETF with @eap-fido.eu

Discussion: external FIDO Servers and FIDO Challenge

- Current Design: Custom FIDO challenge format
  - Binary format (opposed to the JSON-like format in WebAuthn)
  - Challenge exported from TLS keying material
  - Server can send additional challenge parts
- Problem with this design: External FIDO servers are not possible
  - FIDO Servers expect to supply the challenge themselves
  - FIDO challenge signed by FIDO token is expected to be in JSON-Structure defined in WebAuthn (as far as I know)

Pro/Con for FIDO Challenge format change

- Update to WebAuthn-like structure has several disadvantages
  - No cryptographic binding to TLS channel
    - Challenge is generated by FIDO server independent of the TLS keying material
    - May not be a big problem, because the server is generating the challenge and not the client
  - Possibility for Cross-Protocol attacks due to the identical structure of challenge
    - If certificate check is done properly this may not be that bad?
- Aligning Challenge with WebAuthn allows to use FIDO servers without (significant) changes
  - Possibly still changes necessary to allow silent authentication

Discussion/Questions?

- 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