DFN

DEUTSCHES FORSCHUNGSNETZ

draft-janfred-eap-fido-02
Update on EAP-FIDO (or whatever it may be called in the end)

IETF 119 in Brisbane – emu WG | 19.03.2024

Janfred Rieckers | DFN-Verein

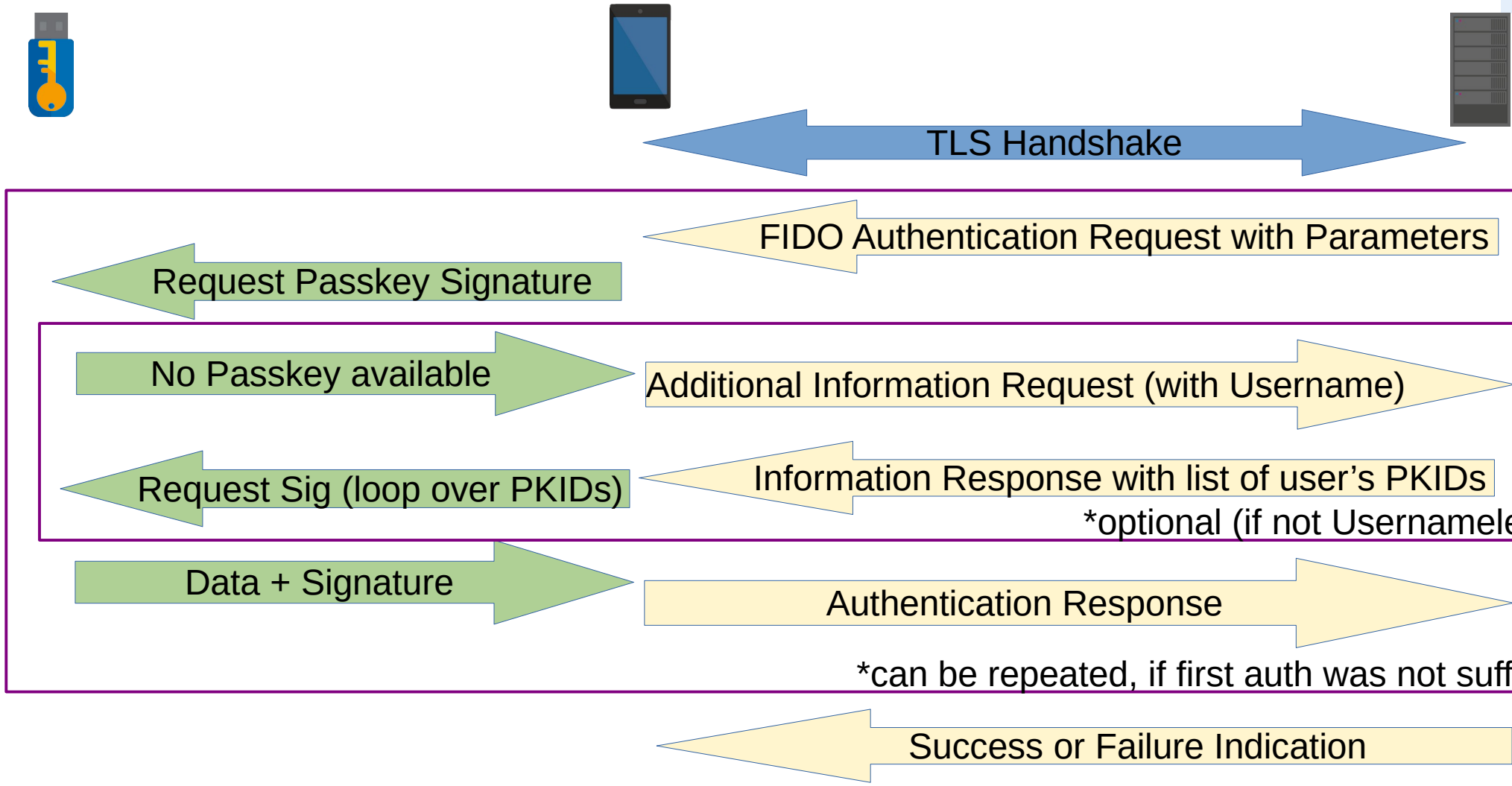
Recap: Background on problems with EAP

- Secure TLS configuration is not easy, users get it wrong constantly
  - „Do not validate“ is the most evil culprit. If you select it, it just works, and users have no idea that they may be broadcasting their credentials to anyone who asks (aka anyone with a rogue AP with the same SSID)
- Passwords are bad
  - Authentication through Knowledge by giving away the Knowledge is the root cause of phishing attacks. If the TLS cert check is broken, a rogue AP can intercept the password
- TLS Client Certificates need to be bootstrapped and they expire.
  - We need a device-specific provisioning mechanism
  - Users need to be reminded that they need to renew their certificate

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 CTAP (v2+)
    - 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 118 (Prague)

- Finally decided on the „One string to rule them all“: FIDO RPID
  - EAP Identity (“outer identity”) is set to *anonymous@<FIDO RPID>*
  - Expected server name (for cert check) is set to *eap-fido-authentication.<FIDO RPID>*

    (Final name may differ, depending on the final name of the protocol)
  - For server-side (non-discoverable) credentials: additional optional field for Identity (Username, „inner identity“)
- Some wordsmithing, updates on the message format following the decision to rely on the FIDO RPID

Upcoming work, next steps

- Proof-of-concept implementation started during hackathon, not finished yet
  - Needed to understand several error conditions that may need a separate error code
- More text around FIDO/CTAPv2 (currently this section is mostly a stub)
- Multiple FIDO signatures? (i.e. when multiple discoverable credentials for the same realm exist?

Open discussion items, moving forward

- Message format
  - CBOR-Maps? Tags? Or TLV again?
- Error transmission
  - Have separate messages for terminal and non-terminal error conditions or use the equivalent of the „critical“ flag?
- Liaison statement from FIDO Alliance?
- We still don’t have a good name… (see link to the HedgeDoc on the ML on March 2nd)

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