

draft-ietf-emu-eap-fido-00

Update on EAP-FIDO (name change coming)

IETF 120 in Vancouver – emu WG | 23.07.2024

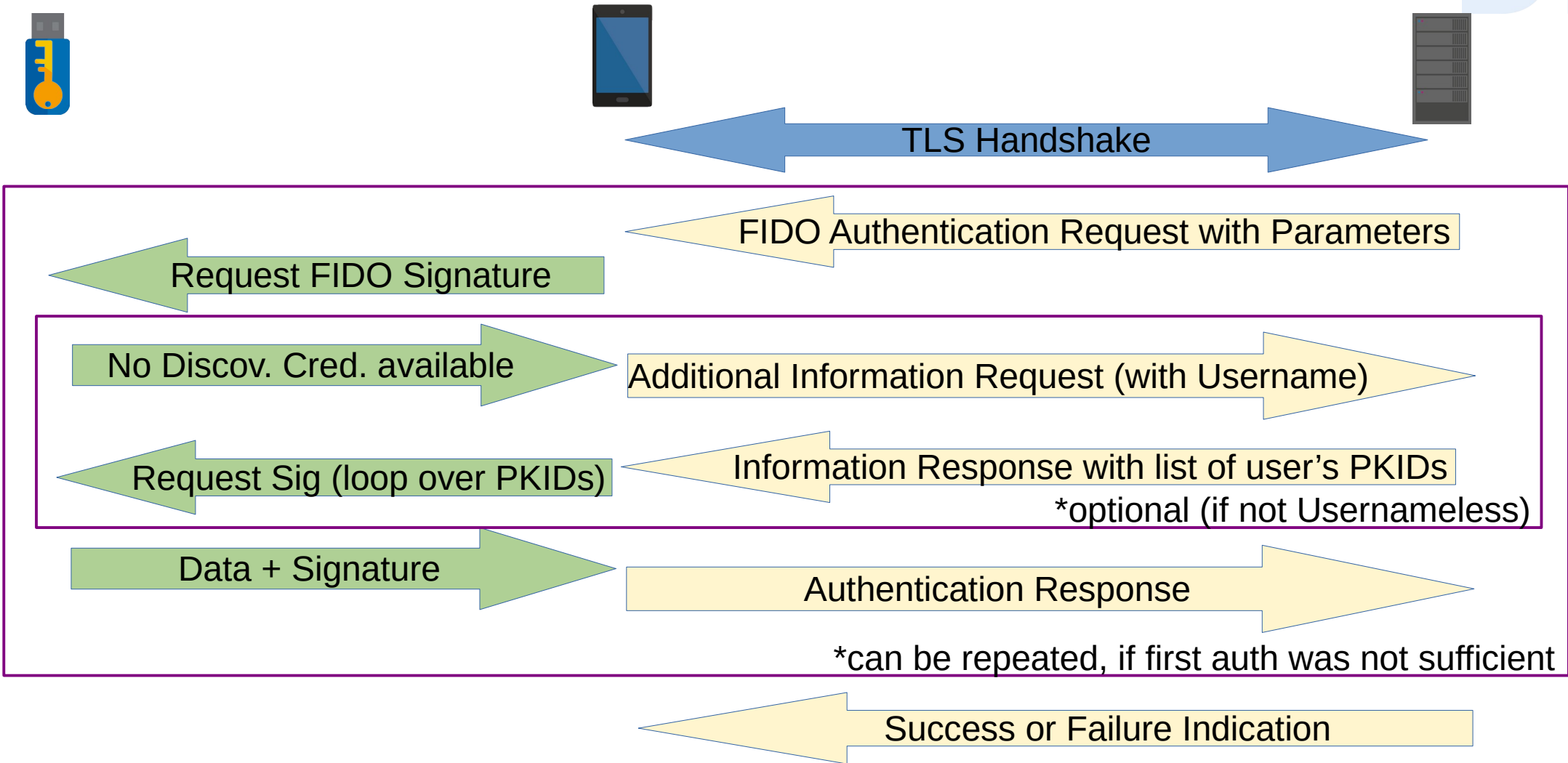
Janfred Rieckers | DFN-Verein

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 119 (Brisbane)

- ▶ First WG draft
- ▶ Small changes in the data format
 - Use numeric keys for standardized authentication requirements (currently user presence/user verification) and string keys for experimental
- ▶ Some minor wordsmithing
- ▶ Most FIDO text is still mainly TODO

Running code

- ▶ Proof-of-concept implementation in hostap (hostapd/wpa_supplicant) is functioning for some specific use cases, not finished yet
 - Needed to understand several error conditions that may need a separate error code
 - Currently only support for Discoverable Credentials, with an sqlite DB in background
 - only works with CTAP clients for now, more implementations are planned
- ▶ Registration is not in scope for the spec, Proof-of-concept code uses a simple web application for FIDO key registration

Raised issues on the ML/last meeting

▶ Crypto agility

- WebAuthn is fixed on SHA-2, we probably shouldn't have a fixed hash algorithm in this spec

▶ Platform Authenticators don't do CTAP

- Specification shouldn't rely only on CTAP, to allow the intended use case with platform authenticators and silent authentication with them
 - Would need implementation effort from OS vendors to add a silent authentication option to their FIDO interface

Next steps – And a name idea

▶ Contact with W3C

- Already got a reply with interest, will meet with some W3C people after this IETF

▶ Name idea to replace „EAP-FIDO“: EAP-NetAuthn

- In relation to „WebAuthn“ for Web context. Uses the same principles. just for network access not for web.
- For UI probably „Use Passkey“ or something similar

Discussion/Questions?

DFN

► 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

