

draft-acme-device-attest

Brandon Weeks

IETF 119

Design goals

- Issuance of client certificates to devices
 - For example: an enterprise issuing client certificates to employee laptops
- Build upon existing attestation schemes and formats
 - Meet platform vendors where they are
 - WebAuthn attestation statement format has robust library support and is widely deployed
 - Not intended to interoperate with RATS
 - Presumably will be supplanted by RATS once adopted by vendors
- Relatively simple & non-exhaustive
 - A protocol that is easy to implement for platforms that already support WebAuthn
 - Not intended to be appealing for vendors that don't already support WebAuthn
 - Not intended for Web PKI

Public implementations

- Clients
 - 🍏: iOS, iPadOS, macOS, and tvOS
 - [acmez](#) (Go library)
- CAs
 - Smallstep

Next steps?