

ACME Client Certificates

Kathleen Moriarty
Dell EMC

3 types to consider

Device

End User

CodeSigning

Device Certificates

- Only real change here from web server certificates are in the CSR
- Could use DNS or IP address mechanisms for auth method
- RFC8555 calls out web server certificates explicitly, some think client certificates are not covered as a result
 - Does this matter?

- Question
 - Should a type be added to distinguish the certificate type or left to the ACME client?

End User Certificates

- Should ACME handle end user certificates?
 - Or leave to efforts like FIDO?

- Authentication types possible:
- Federated Trust Service?
- Risk based authentication

CodeSigning Certificates

- Is identity proofing for less than EV certificates useful?
- EV Certificates typically
 - Require an Account pre-created
 - CAA validation (already optionally included in ACME)
 - Authorization from 1 of 2 administrators
- Would requires a new pre-authorization type
 - Email
 - SMS
 - Something else?