draft-ietf-acme-acme

IETF 100

TODO

~~AD review comments~~

Gen-ART review comments

Resolve “proactive issuance” question

Proactive Issuance - Requirements

General model: Request issuance -> Fulfill authz -> Get certificate

Question: When does CSR* get sent?

1. CSR information at the beginning of the issuance process
    a. For legacy back-end APIs
    b. So that the CA can tell the client what authz to do
2. Don’t require storage of a CSR until after authz is complete
    a. So the CSR needs to be sent after authz
3. Don’t require issuance until someone asks for the certificate (after authz)

General Flow

1. Client sends in the CSR
2. The server sends back the IDs the client needs to prove and authz instructions
3. Client fulfills authzs
4. [The client sends a POST with the CSR]
5. Send a GET to the certificate URL

Do we always do step 4?

Solution Approaches

Always send the CSR twice

- New-order flow has client always send CSR twice
- … even if the CA has cached it

PR #342 (uses “identifiers” instead of CSR)

Benefit: Consistent client logic
Cost: Unnecessary client caching / transmit

Only send twice when the CA needs it

- CA signals to client whether or not it will cache CSRs during the authz flow
- Client caches and retransmits as necessary

PR #350 (uses error code to signal)

Benefit: Only retransmit for frugal CAs
Cost: Branch in client logic

Discuss!