


ACME Renewal Information

draft-ietf-acme-ari-01

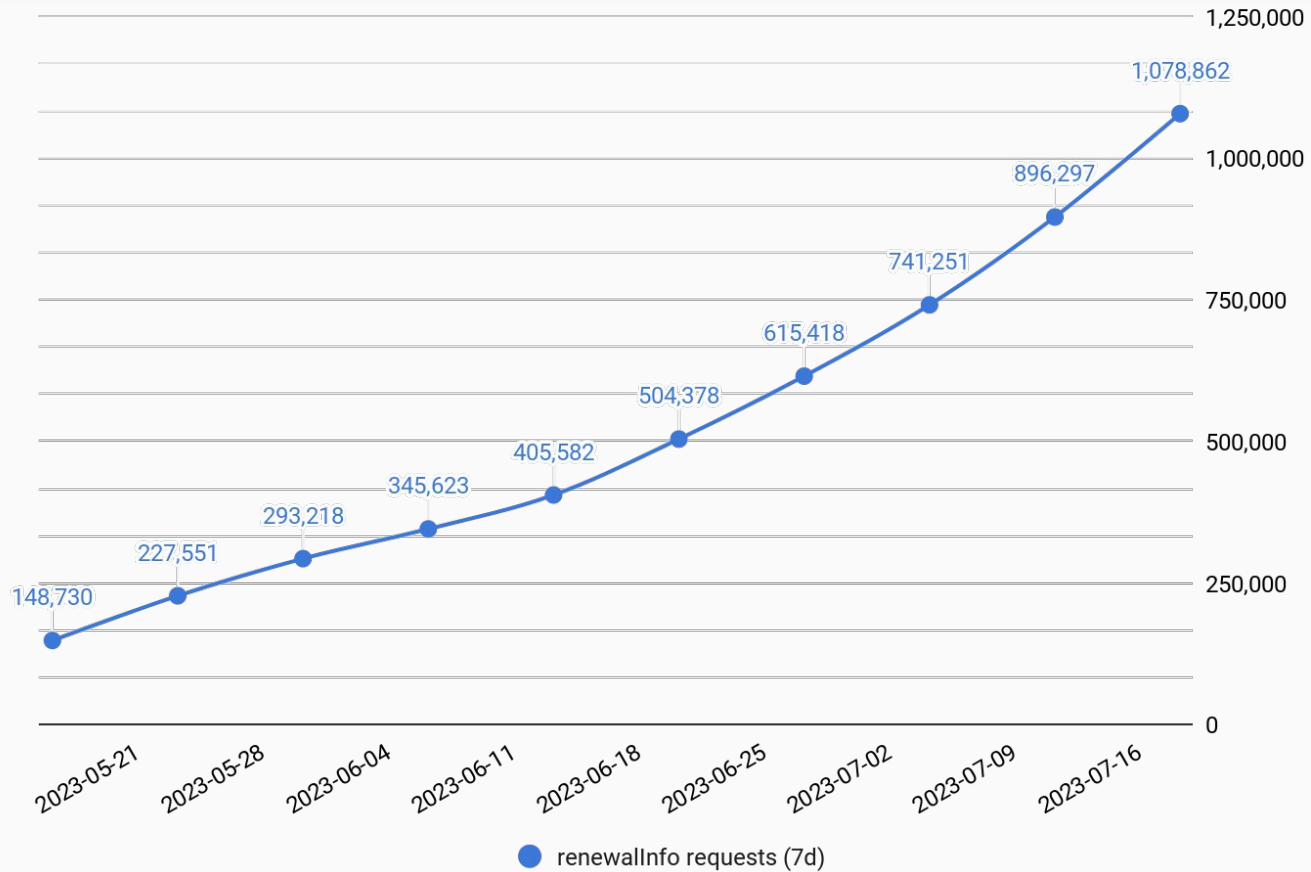
Samantha Frank, Let's Encrypt
IETF 117, 2023-07-24



- No changes to the draft specification
- Fully implemented by Let's Encrypt
- Fully implemented by Google Trust Services
- Under evaluation by Certainly (Fastly)

- Client adoption
 - eggsampler/acme (Go)
 - go-acme/lego (Go)
 - Let's Encrypt is contributing to multiple clients

ARI Endpoint Usage



Open Questions

- Construction of the unique certificate ID
 - OCSP CertID
 - base64url(Authority Key Identifier + Serial)
- Reducing request volume
 - Batch endpoint
 - GET
 - POST-as-GET
 - Include current CertID in newOrder requests
- Simplifying client logic
 - Single timestamp instead of window
 - Bypassing rate limits for renewals during window