ACME Renewal Information

draft-ietf-acme-ari-08

Aaron Gable, Let’s Encrypt
IETF 122, 2025-03-20

Since IETF 121

- Draft -06
  - Sent to IESG for consideration as a Proposed Standard
- Draft -07
  - Rewrote client scheduling requirements and recommendations
  - Added security considerations re: clock skew
  - Many small editorial improvements
  - Sent to IESG ballot
- Draft -08
  - Further improvements to client scheduling
  - Changed some client SHOULDs to MUSTs
  - Many more small editorial improvements
  - Approved by the IESG as a Proposed Standard
  - Sent to the RFC Editors' queue

Thank you for all the reviews and feedback!

- David Dong
- Deb Cooley
- Éric Vyncke
- Geoff Huston
- Jacob Hoffman-Andrews
- Mahesh Jethanandani
- Michael Tüxen
- Murray Kucherawy
- Paul Wouters
- Richard Barnes
- Sabrina Tanamal
- Shawn Emery
- Susan Hares
- Yoav Nir
- Zaheduzzaman Sarker

ACME Profiles

draft-aaron-acme-profiles-00

Aaron Gable, Let’s Encrypt
IETF 122, 2025-03-20

Since IETF 121

- No updates to draft-aaron-acme-profiles-00

- Deployed in Let's Encrypt's staging and production environments
  - Three profiles configured in each

- Implemented in ACME clients:
  - certbot (library / cli)
  - lego
  - eggsampler
  - acmez / certmagic / caddy
  - certifytheweb
  - posh-acme

Next Steps

- Questions / comments / feedback?
- Call for adoption?