26 July 2024

IETF 120 ACME Session

This session is being recorded

Internet Engineering Task Force

Production by Meetecho

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

Note Really Well

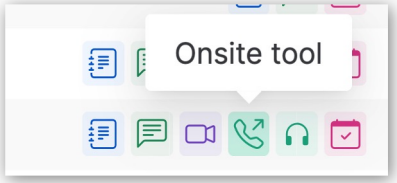
- IETF meetings, virtual meetings, and mailing lists are intended for professional collaboration and networking, as defined in the IETF Guidelines for Conduct (RFC 7154), the IETF Anti-Harassment Policy, and the IETF Anti-Harassment Procedures (RFC 7776). If you have any concerns about observed behavior, please talk to the Ombudsteam, who are available if you need confidentiality to raise concerns confident about harassment or other conduct in the IETF.
- The IETF strives to create and maintain an environment in which people of many different backgrounds and identities are treated with dignity, decency, and respect. Those who participate in the IETF are expected to behave according to professional standards and demonstrate appropriate workplace behavior.
- IETF participants must not engage in harassment while at IETF meetings, virtual meetings, social events, or on mailing lists. Harassment is unwelcome hostile or intimidating behavior—in particular, speech or behavior that is aggressive or intimidates.
- If you believe you have been harassed, notice that someone else is being harassed, or have any other concerns, you are encouraged to raise your concern in confidence with one of the Ombudspersons.

This session is being recorded

IETF 120 Meeting Tips

In-person participants

- Make sure to sign into the session via Datatracker or the QR Code in this session.
- Use Meetecho (usually the “Meetecho lite”) client to:
  - join the mic queue
  - participate in shows of hands
- *Keep audio and video off if not using the onsite version.*



Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session.
- Use of a headset is strongly recommended.

Resources for IETF 120 Vancouver

- Agenda
  https://datatracker.ietf.org/meeting/agenda
- Meetecho and other information:
  https://www.ietf.org/how/meetings/preparation
- If you need technical assistance, see the Reporting Issues page:
  http://www.ietf.org/how/meetings/issues/

Agenda

Agenda

- Technical difficulties, Agenda bashing, etc – 5 minutes
- Document Status – Chairs – 10 minutes

- DTN Node ID Validation – Sipos – 15 minutes
- ACME Renewal Information – Gable – 15 minutes
- ACME Profiles – Gable – 15 minutes

Document Status

Document Status (1/3)

- No new RFCs since September ☹️
- ACME Renewal Information
  - Version -04 published at the end of May
  - Have presentation in this session

Document Status (2/3)

- ACME DTN Node ID
  - No new version since IETF 119
  - Has been stuck for ages waiting for dtn-bpv7-admin-iana
  - We may have good news on that…

- ACME Onion – no new version since before IETF 119
- ACME Device Attest – no new version since before IETF 119
- ACME Scoped DNS Challenges - ditto

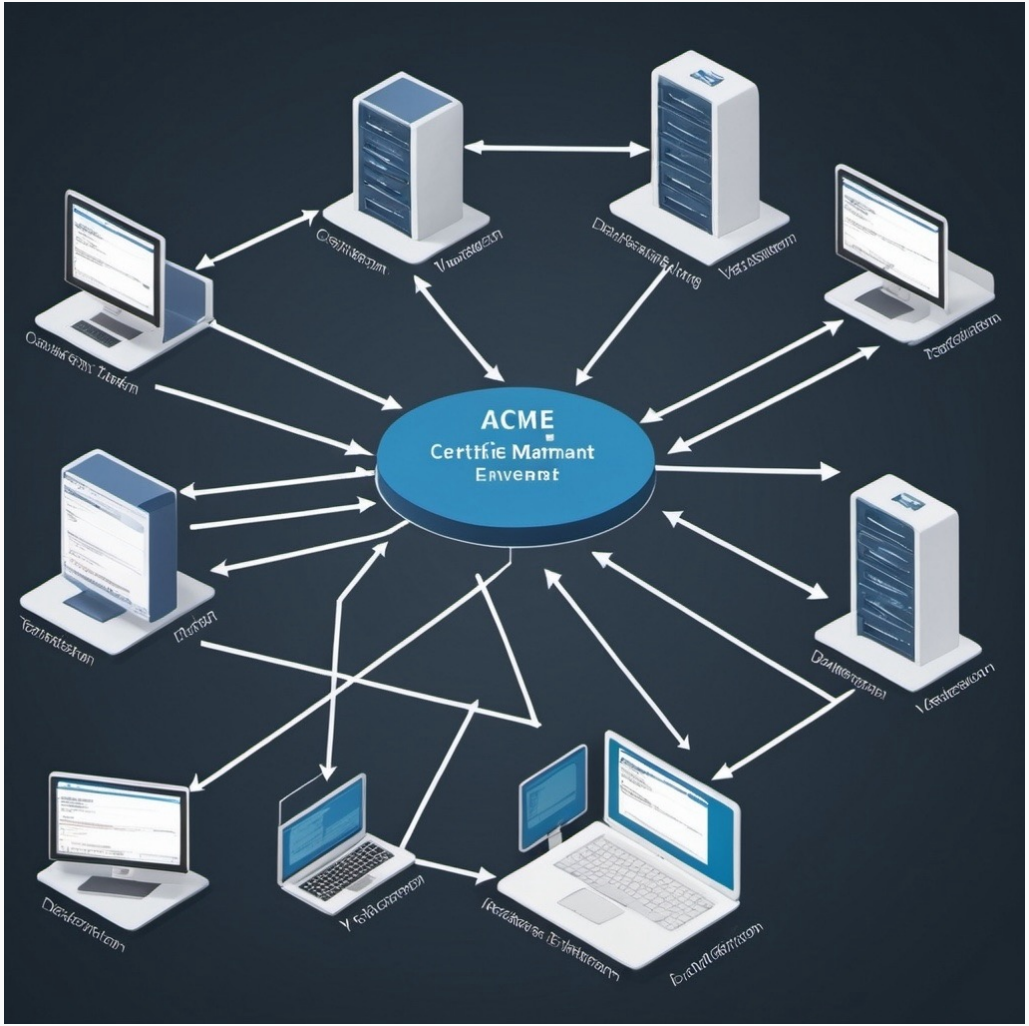
Document Status (3/3)

- ACME Integrations
  - Has been in the RFC Editor queue for 377 days.
  - Waiting for draft-ietf-anima-brski-cloud
    - In state **AD Evaluation::Revised I-D Needed** for 189 days.
  - Waiting for draft-ietf-lamps-rfc7030-csrattrs
    - In state **Revised I-D Needed - Issue raised by WGLC** for 16 days.
  - Some common authors on these three documents.
- ACME-Client hasn't been updated in a year – dead?

Presentations w/o slides

ACME - DTN Node Id

- Brian Sipos



Presentations with slides

ACME Renewal Information

draft-ietf-acme-ari-04

Aaron Gable, Let’s Encrypt
IETF 120, 2024-07-26

Since IETF 119

- Draft -04 published as described at IETF 119
- No changes since then

- 10+ client implementations
  - lego, tailscale, certify the web, caddy, certmagic, acmez, eggsampler, acme4j, win-acme, ansible, acmecert, posh-acme
- 3+ server implementations
  - 2+ more promised in Bugzilla incident reports

Open Questions

- Servers reject new-order requests for many reasons.
- Should “because you specified a predecessor which is already replaced” be uniquely recognizable?

- Working Group Last Call?

Proposal: ACME Profiles

draft-aaron-acme-profiles-00 eventually

Aaron Gable, Let’s Encrypt
IETF 120, 2024-07-26

The Problem

- new-order has few knobs:
  - `notBefore`
  - `notAfter`
  - `identifiers`
- finalize CSR is unwieldy
  - Too late
  - Too untrusted
  - Too fine-grained
  - Difficult for clients to manipulate

The Solution

- “Profiles” – CA-curated collections of certificate attributes

- Pros:
  - Simple for clients to implement
  - Simple for site operators to configure

- Cons:
  - No dynamic profile negotiation

Concrete Proposal

- Augment the directory:

```
GET /directory HTTP/1.1

{
  "newAccount": "https://api.example.ca/acme/new-account",
  "meta": {
    "profiles": {
      "legacy": "The same profile you know and love",
      "modern": "https://example.ca/profiles#tls-server"
    }
  },
  ...,
}
```

Concrete Proposal

- Augment the order object:

```
POST /acme/new-order HTTP/1.1

{
  "protected": base64url(...),
  "payload": base64url({
    "profile": "modern",
    "identifiers": [{"type": "dns", "value": "example.org"}],
  }),
  "signature": "H6ZXtGjTZyUnPeKn...wEA4TklBdh3e454g"
}
```

Status

- Already implemented by Let's Encrypt / Boulder
- Profile controls:
  - Validity period
  - Inclusion of Common Name
  - Inclusion of Subject Key ID
  - Inclusion of TLS Client Auth EKU
  - Inclusion of keyEncipherment KU (for RSA certs)
- Next steps:
  - Control lifetime of ACME order / authorization objects
  - Client implementations
  - Standardization

AOB