ACME @ IETF 114

28 July 2022

This session is being recorded

IETF 114 Philadelphia
hosted by

COMCAST

NBCUniversal

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:

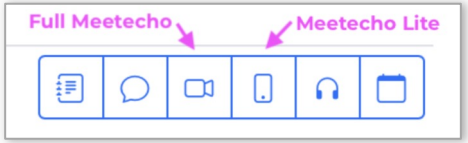
- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

This session is being recorded

IETF 114 Meeting Tips

In-person participants

- Make sure to sign into the session using the Meetecho (usually the “Meetecho lite” client) from the Datatracker agenda
- Use Meetecho to join the mic queue
- *Keep audio and video off if not using the onsite version*
- **Wear masks unless actively speaking at the microphone.**



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 114 Philadelphia

- Agenda
  https://datatracker.ietf.org/meeting/agenda
- Meetecho and other information:
  https://www.ietf.org/how/meetings/114/preparation
- If you need technical assistance, see the Reporting Issues page:
  http://www.ietf.org/how/meetings/issues/

Agenda

- Note Well, Technical difficulties, and Administrivia
- Document Status (chairs)
- Current work items:
  - draft-ietf-acme-dtnodeid-09 (Sipos)
  - draft-aaron-acme-ari (Gable)
- (Potential) new work:
  - draft-bweeks-acme-device-attest (Weeks)
- AOB

Document Status

- No new RFCs ☹
- acme-authority-token
  - Has a discuss from Ben Kaduk since 27-Nov-2021
  - New version -08 from this month
  - What to do?
- acme-client
  - New version -05 from April
  - Light discussion on the ML

Document Status

- authority-token-tnauthlist
  - Current version from 26-Mar-2021
  - Has 3 outstanding DISCUSS-es
  - Revised I-D needed
- dtnnodeid
  - Current version from just before IETF 113
  - Waiting for Writeup::External Party since 20-Mar-2022
  - Have a presentation today.

Document Status

- Integrations
  - Went through WGLC with sparse discussion
  - Ready to go ahead?
- Subdomains
  - Just finished WGLC
- ARI
  - Attempted WG adoption
  - Crickets...

draft-ietf-acme-dtnnodeid

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

ACME DTN Node ID Validation

IETF 114 ACME WG

Brian Sipos
JHU/APL

Current Status of Draft

- Latest is https://www.ietf.org/archive/id/draft-ietf-acme-dtnnodeid-09.html
- Changes since -06:
  - Added more detailed explanation of DTN terminology to explain what this validation covers (Administrative Endpoint ID) and what it does not (other types of Endpoint ID).
  - Separated “id-chal” “token-chal” and “token-bundle” to avoid overlaps in purpose and to behave more like RFC 8823 (email validation).
  - Added digest algorithm agility based on COSE example encoding.
    - SHA-256 is still mandatory-to-implement for interoperability.
  - Fixed typo in Section 3.1 introduced in earlier -06 edit
  - Removed old identifier name “uri” and replaced with correct “bundleEID”.
  - Example bundles now use proper indefinite-length array framing.
- Known issues remaining:
  - The COSE Hash Algorithms document is still in AUTH48 status.

draft-aaron-acme-ari

ACME ARI Extension

`draft-aaron-acme-ari-03`

Aaron Gable, ISRG

Since IETF 113

- Provided clearer motivation in the Introduction
- Clarify suggested renewal algorithm
- Fix minor typos

- Call for adoption

Renewal Time Algorithm

Conforming clients **MUST** attempt renewal at a time of their choosing based on the suggested renewal window. The following algorithm is **RECOMMENDED** for choosing a renewal time:

1. Select a uniform random time within the suggested window.
2. If the selected time is in the past, attempt renewal immediately.
3. Otherwise, if the client can schedule itself to attempt renewal at exactly the selected time, do so.
4. Otherwise, if the selected time is before the next time that the client would wake up normally, attempt renewal immediately.
5. Otherwise, sleep until the next normal wake time, re-check ARI, and return to Step 1.

In all cases, renewal attempts are subject to the client's existing error backoff and retry intervals.

Next Steps

- Update Let’s Encrypt’s implementation to match latest draft
- Address any further feedback from call for adoption

draft-bweeks-acme-device-attest

draft-bweeks-acme-device-attest-00

Brandon Weeks, Google

tl;dr

- Describes how WebAuthn attestation statements can be included in a challenge response payload to attest to the identity of the requesting device along with the key generation parameters.
- Primary use case is issuing client certificates.

Why ACME?

- SCEP, despite its flaws, remain the primary certificate enrollment protocol used for client certificate enrollment.
- ACME has an extensible design that permits inclusion of attestation with few changes.
- Ubiquitous library support.

Why now?

- Attestation schemes have matured and become ubiquitous:
  - Android Key Attestation (Android)
  - Managed Device Attestation (iOS, macOS soon?)
  - Chrome Verified Access (Chrome OS)
  - RATS Entity Attestation Token (eventually?)
  - Trusted Platform Module (Linux, Windows)

WebAuthn attestation statement format usage

- In the wild
  - Apple App Attest
  - WebAuthn :)
- IETF drafts
  - draft-fossati-tls-attestation-00 (tls)
  - draft-wallace-lamps-key-attestation-ext-00 (lamps)
- Ubiquitous library support for CBOR, COSE, and WebAuthn.

ACME extension

- device-attest-01 challenge
  - Challenge response payload contains the attestation statement, instead of an empty JSON object.
  - Key authorization is used as the WebAuthn nonce.
- Identifiers
  - permanent-identifier (RFC 4043)
  - hardware-module (RFC 4108)
- EAB for pre-authorization to the CA

Implementations

- Demonstration CA / client
  - https://github.com/brandonweeks/acme-device-attest-demo
    - Upstream: https://github.com/smallstep/certificates/pull/977
- iOS 16
  - https://developer.apple.com/videos/play/wwdc2022/10143

Open questions

- Is this the right document to specify how key properties should be reflected in issued client certificates?
- Verification procedures and trust anchor selection is complex and poorly specified. Where should the procedures be specified?

AOB