ACME @IETF-104

Rich Salz

Yoav Nir

27-Mar-2019

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)

Agenda

- Blue Sheets, agenda bashing, scribes
- Status (chairs)
- STAR (Yaron)
- Device Attestation (Rifaat)
- Client Certificates (Kathleen)
- TNAuth (Jon)
- Open Mic

Status – RFC 8555 is out!

Internet Engineering Task Force (IETF)
Request for Comments: 8555
Category: Standards Track
ISSN: 2070-1721

J. Hoffman-Andrews
EFF
D. McCarney
Let's Encrypt
J. Kasten
University of Michigan
March 2019

Automatic Certificate Management Environment (ACME)

Abstract

Public Key Infrastructure using X.509 (PKIX) certificates are used for a number of purposes, the most significant of which is the authentication of domain names. Thus, certification authorities (CAs) in the Web PKI are trusted to verify that an applicant for a certificate legitimately represents the domain name(s) in the certificate. As of this writing, this verification is done through a collection of ad hoc mechanisms. This document describes a protocol that a CA and an applicant can use to automate the process of verification and certificate issuance. The protocol also provides facilities for other certificate management functions, such as certificate revocation.

RFC 8555 – Some Stats

- 19 WG draft versions + 5 individual draft versions
- 50 months from individual -00 to RFC (42 from WG -00 version)
- 36 pages in individual -00 ; 95 pages in the RFC

Status — Others

- First version of draft-ietf-acme-star-delegation. Please read.
- New revisions of:
  - Auth / tnAuth: versions ~~-02~~ -03 of both. Please read and comment.
  - CAA-06 (in AD Evaluation)
  - ACME-IP-05 (in AD Evaluation)
- No new revision of smime and email-tls (expired).
  - Alexey promises it will be updated for next time.
- No new revision of ACME-TLS-ALPN, which is in state AD Evaluation::Revised I-D Needed since 24-Dec.

Presentations