SHORT-TERM, AUTOMATICALLY-RENEWED (STAR) CERTIFICATES

draft-ietf-acme-star-05

Thomas Fossati, **Yaron Sheffer**, Diego Lopez

IETF-104, Prague

SUMMARY

- We requested publication, received an extensive AD review from Eric Rescorla – thank you!
- Published as -05

DETAILS

- Clarified timing of certificate issuance with a more formal treatment and a detailed example
  - A new section, Computing *notBefore* and *notAfter* of STAR Certificates
  - Added an explicit parameter for predating, based on client's knowledge of potential time skew
- Authenticated GET opens up enumeration attacks and correlation to accounts, added requirement to use Capability URLs
- A few more minor edits, reference updates

NEXT STEPS

- We suggest to proceed with publication