ACME STAR

draft-ietf-acme-star-03

IETF 101

draft-ietf-acme-star@ietf.org

Changes since Singapore (1)

- Operational considerations
  - Define "short-term" for the web use case (equivalency with OCSP "must-staple"): recommend renewal every 4 days
  - Clock skew considerations based on CCS'17 paper "Where the Wild Warnings Are: Root Causes of Chrome HTTPS Certificate Errors": allow pre-dating 5-7 days
  - CT Log notes, based on online and f2f discussion in Singapore at the ACME, TRANS and STAR side-meeting: "most likely not a problem but, if it was, it's for CT to solve it."

Changes since Singapore (2)

- Added security considerations, mostly around the increased DoS surface & related mitigations
- Slight change in terminology, as suggested by Jon Peterson: s/domain name owner/identity owner/ to mark the fact that short-term auto-renewal based on ACME is orthogonal to the identity type that is used in the subject

Ready for WGLC ?

- Editors think -03 is ready for WGLC
- Thoughts?