Considerations For Using Short Term Certificates

draft-nir-saag-star-01

Authors:

Y. Nir Dell EMCT.

Fossati Nokia

Y. Sheffer Intuit

T. Eckert Huawei

Presented by:
Max Pritikin

Section 3: Use cases

- Predominately described for ANI

NOTICE that

- Infrequently run code is hard to trust
- The interactions of CA, CRL Distribution Point, OCSP etc are complex with many edge conditions

Section 4: Operational Considerations

- Lifetime and Renewal
  - “Short” = hours
  - Automated via BRSKI then EST/ACME
  - NOTE: S4.5 conflates BRSKI & EST/ACME for renewal
- Availability of CA
  - New(ish)
  - Not substantially different than OCSP server being online
  - Harder than CRL distribution Point availability
- Clock Skew
  - This is an issue with nonceless OCSP or CRL so needs to be considered anyway
- Certificate Transparency
  - More data to log and sift through
  - Unless you consider that OCSP responses should be tracked too?

BRSKI Vouchers are short lived

- Section 6.1: “Renewals instead of Revocations”

https://tools.ietf.org/html/draft-ietf-anima-voucher-07#section-6.1

“re-issuing the voucher should be a lightweight process, as it ostensibly only updates the voucher's validity period. With this approach, there is only the one artifact, and only one code path is needed to process it, without any possibility for a pledge to choose to skip the revocation status check because, for instance, the OCSP Responder is not reachable.”