EST Renewal Info

Rifaat Shekh-Yusef, Michael Richardson, Mike Ounsworth

Goals / Problem Statement

- When you have a cert, you know when it will expire (`notAfter`).
- You don't know when you are *allowed* to renew it (50% lifetime? 30 days?).
- Often in IoT, it's useful to have a dashboard of certs eligible for early renewal.
  - This can be used to know if some devices have failed to renew in a timely fashion
- Some devices might be fully air-gapped/offline, or might have time limited connectivity (online only via special arrangement, such as when a technician visits).
  - Knowing if the device should/could renew at that time, or should wait for next scheduled visit is useful
- ACME recently added a mechanism for this – RFC9773 ACME Renewal Information (ARI).
- *We want to port ACME ARI as verbatim as practical into RFC7030/EST.*

Next Steps

No detailed draft yet, but should be straightforward to port the ACME ARI (RFC9773) content to fit EST.

Questions:

- LAMPS WG feeling on this? 👍/👎
- If anyone wants to be involved, please contact Rifaat, MCR, or MikeO.

Detailed use cases follow

Thanks!

Use Case 1

- Some customers want device identity CAs (want) to issue very short-lived certificates (few days) to devices.
    - More details forthcoming, as they are “declassified”/”anonymized”
- Devices are expected to renew their certificate before the expiry.
    - Some customers suggest 50% of certificate life-time
        - On a 4-day certificate, that’s too soon

Use Case 2 - long lived certificates, frequently renewed

- CA Issues long-lived certificates (few years) to devices
  - Certificates expiring in the field is a major anxiety for many deployments
- Devices are expected to discover the renewal details from the CA
  - CA may need to change things: key size, algorithm choices (SHA1,2,3..)
  - Knowing a device will return in a predictable fashion allows for less criticality around choices
- For instance, a three year lifetime, and devices should renew within the first year
  - Don’t come back early, please don’t come back late
  - Always have a two year runway
- Like ACME, there is a concern with flooding the CA
- Also allows for replacement of **subordinate** CA
  - Enables clients to be changed from say, “Accounting” -> “Finance” subordinate

Does renewal include other information?

- where to go to renew?
  - rebalancing/reselling of CA services
  - when a CA sells off a category of clients to another provider