ACME ARI Extension

draft-aaron-acme-ari-03
Aaron Gable, ISRG
Since IETF 113

- Provided clearer motivation in the Introduction
- Clarify suggested renewal algorithm
- Fix minor typos

- Call for adoption
Renewal Time Algorithm

Conforming clients **MUST** attempt renewal at a time of their choosing based on the suggested renewal window. The following algorithm is **RECOMMENDED** for choosing a renewal time:

1. Select a uniform random time within the suggested window.
2. If the selected time is in the past, attempt renewal immediately.
3. Otherwise, if the client can schedule itself to attempt renewal at exactly the selected time, do so.
4. Otherwise, if the selected time is before the next time that the client would wake up normally, attempt renewal immediately.
5. Otherwise, sleep until the next normal wake time, re-check ARI, and return to Step 1.

In all cases, renewal attempts are subject to the client's existing error backoff and retry intervals.
Next Steps

- Update Let’s Encrypt’s implementation to match latest draft
- Address any further feedback from call for adoption