# EST Renewal Info

IETF124, LAMPS WG
Rifaat  Shekh-Yusef, Michael Richardson, Mike Ounsworth

# Goal – Bring ACME ARI to EST

- ACME Renewal Information (ARI) was recently published as RFC 9773.
- It allows the ACME server to provide suggestions to ACME clients as to when they should attempt to renew their certificates.

- The EST protocol would benefit from having a similar extension registered for EST.
- This document attempts to port RFC 9773 to EST with as few changes as possible.

# Goal

Allow the EST Server to provide information to EST Clients about the recommended certificate renewal period.

The EST Server might also provide further information about other related issues:

- When should the EST Client raise an alarm if it fails to renew a certificate after some specific period.
- Proper backoff mechanism to ease the load on the EST server and to reduce the amount of logs on the EST client.

# EST Extension

This document introduces a new HTTP endpoint to extend RFC7030:

/.well-known/est/**renewal-info/<certificate-id>**

The **<certificate-id>** segment contains the unique id of the certificate.

# Example of Renewal Info Request

GET /.well-known/est/renewal-info/<certificate-id>

# Example of Renewal Info Response

HTTP/1.1 200 OK

Content-Type: application/json

Retry-After: 21600


```
{
  "suggestedWindow": {
    "start": "2025-12-04T04:00:00Z",
    "end": "2025-12-05T04:00:00Z" }
}
```

# OPEN ISSUE - Should I renew now?

https://github.com/mcr/lamps-rfc7030-renewal-recommendation/issues/1

Why do we need this?

If we introduce a new endpoint for this, how would that be different from an attempt to renew and for the server to tell the client not now?

# OPEN ISSUE - Client and IoT end-system certificates

https://github.com/mcr/lamps-rfc7030-renewal-recommendation/issues/11

EST is used within Enterprises, (it's core for BRSKI), and so there might be orders of magnitude more client systems involved.

Yes, of course public LE ACME is way bigger, but the number of *client* certificates per "account" is smaller.

EST does not have accounts, but particularly if the EST server is outsourced, given NAT44, controls might exist on a per-IP basis, and/or there could be a layer of local RA that adds an account-like mTLS to the process.

The question is: are there any additional considerations here?

# OPEN ISSUE - General Renewal Info

https://github.com/mcr/lamps-rfc7030-renewal-recommendation/issues/12

Should we support a general renewal info, in the absence of a certificate renewal info, such as:

GET /.well-known/est/renewal-info

# OPEN ISSUE - Reference or Copy RFC9773

How much to point at 9773, how much to copy/quote, and how much to make our own?

# Adoption

Should the WG adopt this document?