LAMPS Working Group
Internet-Draft
Intended status: Standards Track
Expires: 6 April 2026

R. Shekh-Yusef
Ciena
M. Richardson
Sandelman Software Works
M. Ounsworth
Entrust Limited
3 October 2025

Certificate Renewal Recommendations for Enrollment over Secure Transport draft-yusef-lamps-rfc7030-renewal-recommendation-03

Abstract

This document describes an extension to RFC7030, Enrollment over Secure Transport to give an indication to a end-entity device when it should start attempting to renew its certificates.

Prior art is that client decides, with a typical recommmendation to start when the remaining lifetime of the certificate is at the 50% point. As typical certificate lifetimes are reduced from years to fractions of a year, the 50% may be far too early, and this document provides a way to give alternate advice.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-yusef-lamps-rfc7030-renewal-recommendation/.

Discussion of this document takes place on the lamps Working Group mailing list (mailto:spasm@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/spasm/. Subscribe at https://www.ietf.org/mailman/listinfo/spasm/.

Source for this draft and an issue tracker can be found at https://github.com/mcr/rfc7030-renewal-recommendation.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

This Internet-Draft will expire on 6 April 2026.

Copyright Notice

Table of Contents

1. Introduction

[RFC9773], Section 1 explains why certificate lifetimes and renewal times need more deterministic control in the ACME [RFC8555] ecosystem. Similar arguments apply to the [RFC7030] ecosystem.

This document extends [RFC7030] to add support for renewal information, by adding a new entry to the HTTP URIs for Control list defined in [RFC7030], Section 3.2.2

This mechanism enables EST servers to provide suggested detailed renewal operations to EST clients.

The /renewal-info URI is added, as an OPTIONAL operation, to the table in figure 5 in section 3.2.2 of [RFC7030].

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Protocol Details

3.1. Renewal Information Request

To retrieve the renewal information, the EST client uses the following HTTP request-line:

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

The request includes a unique identifier for the certificate in question. The unique identifier is constructed by concatenating the base64url encoding [RFC4648] of the keyIdentifier field of the certificate’s Authority Key Identifier (AKI) [RFC5280] extension, the period character ".", and the base64url encoding of the DER-encoded Serial Number field (without the tag and length bytes). All trailing "=" characters MUST be stripped from both parts of the unique identifier.

Thus, the full request URL is constructed as follows (split onto multiple lines for readability), where the "||" operator indicates string concatenation:

```
url = /.well-known/est/renewal-info
  || '/'
  || base64url(AKI keyIdentifier)
  || '.'
  || base64url(Serial)
```

3.2. Renewal Information Response

The structure the EST RenewalInfo object is as follows:

suggestedWindow (object, required): A JSON object with two keys, "start" and "end", whose values are timestamps, encoded in the format specified in [RFC3339], which bound the window of time in which the CA recommends renewing the certificate.

For example:

```
HTTP/1.1 200 OK
Content-Type: application/json
Retry-After: 21600

{
  "suggestedWindow": {
    "start": "2025-01-02T04:00:00Z",
    "end": "2025-01-03T04:00:00Z"
  }
}
```

3.2.1. Base64 Not Used

[RFC7030] mistakenly declared that all content would be base64 encoded. [RFC8951] clarifies that the content is to be base64 encoded, whether or not there is a Content-Transfer-Encoding header present. It further clarifies that future extensions (such as this document) will not use base64 encoding. The response detailed above is not base64 encoded.

4. Renewal Operations

Clients MUST attempt renewal at a time of their choosing based on the suggested renewal window, obtained in the previous step.

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 time indicated by the Retry-After header and return to Step 1.

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

A RenewalInfo object in which the end timestamp equals or precedes the start timestamp is invalid. Servers MUST NOT serve such a response, and clients MUST treat one as though they failed to receive any response from the server (e.g., retry at an appropriate interval, renew on a fallback schedule, etc.).

4.1. Fetching Schedule

The advice in [RFC9773], Section 4.3 applies:

Clients SHOULD fetch a certificate's RenewalInfo immediately after issuance.

During the lifetime of a certificate, the renewal information needs to be fetched frequently enough that clients learn about changes in the suggested window quickly, but without overwhelming the server. This protocol uses the Retry-After header [RFC9110] to indicate to clients how often to retry. Note that in other HTTP applications, Retry-After often indicates the minimum time to wait before retrying a request. In this protocol, it indicates the desired (i.e., both requested minimum and maximum) amount of time to wait.

Clients MUST NOT check a certificate's RenewalInfo after the certificate has expired. Clients MUST NOT check a certificate's RenewalInfo after they consider the certificate to be replaced (for instance, after a new certificate for the same identifiers has been received and configured).

5. Privacy Considerations

A very short certificate lifetime renewal time will cause clients to communicate with the EST Registrar more frequently.

EST connections for renewals typically make use of mutually authenticated TLS. When the client certificate being an IDevID, or the last issued certificate, often an LDevID, there is potential to disclose identities during this connection when using TLS 1.2.

TLS 1.3 does not suffer from this problem, and it’s use is RECOMMENDED as per [I-D.ietf-uta-require-tls13]

6. Security Considerations

Not sure what yet.

7. IANA Considerations

Might need a header allocation

8. Acknowledgements

Many bits of text are taken from [RFC9773].

9. Changelog

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, DOI 10.17487/RFC3339, July 2002, <https://www.rfc-editor.org/info/rfc3339>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/info/rfc4648>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <https://www.rfc-editor.org/info/rfc7030>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8951] Richardson, M., Werner, T., and W. Pan, "Clarification of Enrollment over Secure Transport (EST): Transfer Encodings and ASN.1", RFC 8951, DOI 10.17487/RFC8951, November 2020, <https://www.rfc-editor.org/info/rfc8951>.

10.2. Informative References

[I-D.ietf-uta-require-tls13] Salz, R. and N. Aviram, "New Protocols Using TLS Must Require TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-uta-require-tls13-12, 14 April 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-uta-require-tls13-12>.

[RFC8555] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019, <https://www.rfc-editor.org/info/rfc8555>.

[RFC9773] Gable, A., "ACME Renewal Information (ARI) Extension", RFC 9773, DOI 10.17487/RFC9773, June 2025, <https://www.rfc-editor.org/info/rfc9773>.

Authors' Addresses

Rifaat Shekh-Yusef
Ciena
Email: rifaat.s.ietf@gmail.com

Michael Richardson
Sandelman Software Works
Email: mcr+ietf@sandelman.ca

Mike Ounsworth
Entrust Limited
Email: mike.ounsworth@entrust.com