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

R. Shekh-Yusef
Ciena
M. Richardson
Sandelman Software Works

5 July 2025

Certificate Renewal Recommendations for Enrollment over Secure Transport
draft-yusef-lamps-rfc7030-renewal-recommendation-00

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 will expire on 6 January 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.

(Do the ecosystems differ in significant ways? Probably. How much to explain)

Is this as much about client certificates and IoT certificates?

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

A new magic header will be returned during RFC7030 certificate enrollment, whether using simpleenroll, or fullcmc.

4. Privacy Considerations

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

EST connections 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, the client certificate details will be revealed. TLS 1.3 does not suffer from this problem, and it’s use is RECOMMENDED as per [I-D.ietf-uta-require-tls13]

5. Security Considerations

Not sure what yet.

6. IANA Considerations

Might need a header allocation

7. Acknowledgements

Hello.

8. Changelog

9. References

9.1. 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>.

[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>.

9.2. 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