Transport Layer Security
Internet-Draft
Intended status: Informational
Expires: 28 August 2026

R. Barnes
Cisco

24 February 2026

Stop Doing Cryptographic Algorithm Drafts when Email to IANA is All You Need
draft-barnes-tls-this-could-have-been-an-email-00

Abstract

People keep pitching drafts to the TLS Working Group where the only thing the draft does is register a code point for a cryptographic algorithm. Stop doing that. It's unnecessary. Write an email to IANA instead.

About This Document

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

The latest revision of this draft can be found at https://bifurcation.github.io/no-more-crypto/draft-barnes-tls-this-could-have-been-an-email.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-barnes-tls-this-could-have-been-an-email/.

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

Source for this draft and an issue tracker can be found at https://github.com/bifurcation/no-more-crypto.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

There used to be a grand tradition of debating the merits of cryptographic algorithms in the TLS working group. Over time, folks realized that this was not a productive use of the WG's time. The typical TLS WG participant is not a cryptographer, and the cryptographic choices of TLS users are typically dictated by other factors than the opinion of the TLS WG.

As a result, [RFC8447] loosened the registration policy on the TLS registries to Specification Required, with a very limited carve-outs related to the "Recommended" column. As a result, anyone can register a code point for a cryptographic algorithm with a stable public specification, without having to convince the TLS WG of anything. Registration is as simple as one email to iana@iana.org (mailto:iana@iana.org).

This document proposes that the TLS WG adopt a restrictive policy that if the only thing a document does could be done without the WG, that document will not be adopted.

2. Conventions and Definitions

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. When Are Crypto Documents OK?

The registry policies in [RFC8447] define a few specific things that require working group action.

* Initial registration with Recommended=Y

* Changing the value of the Recommended column to "Y" or "D" from something else

* Changing the value of the Recommended column from "Y" or "D" to something else

Unless a document does one of these things it MUST NOT be adopted by the WG. Even if there are additional technical details to be specified, the proponents can publish their own specification; even an individual -00 Internet-draft meets IANA’s criteria for a stable, public specification.

For example:

* [I-D.ietf-tls-mlkem] and [I-D.ietf-tls-mldsa] define technical details, but do not request Recommended=Y. The authors could have simply published these details on their own (e.g., in an individual Internet-draft) and requested code points.

* [I-D.reddy-tls-slhdsa] simply registers SLH-DSA code points, pointing to the existing FIPS documents for all technical details. Nonetheless, it has consumed a significant amount of WG time, including multiple challenges and appeals.

Authors that just want to register a code point should skip the working group and go directly to IANA. It's easier, it's faster, and it won't waste a bunch of other folks' time in the working group.

4. Security Considerations

The policy proposed in this document has no impact on security. The registry policies already allow any algorithm with a specification to be registered. Let's just not spend the WG's time debating things that the WG doesn't need to opine on.

5. IANA Considerations

This document has no IANA actions. Ironically.

6. References

6.1. 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/rfc/rfc2119>.

[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/rfc/rfc8174>.

[RFC8447] Salowey, J. and S. Turner, "IANA Registry Updates for TLS and DTLS", RFC 8447, DOI 10.17487/RFC8447, August 2018, <https://www.rfc-editor.org/rfc/rfc8447>.

6.2. Informative References

[I-D.ietf-tls-mldsa] Hollebeek, T., Schmieg, S., and B. Westerbaan, "Use of ML-DSA in TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-mldsa-01, 26 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-mldsa-01>.

[I-D.ietf-tls-mlkem]
Connolly, D., "ML-KEM Post-Quantum Key Agreement for TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-mlkem-07, 12 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-mlkem-07>.

[I-D.reddy-tls-slhdsa]
Reddy.K, T., Hollebeek, T., Gray, J., and S. Fluhrer, "Use of SLH-DSA in TLS 1.3", Work in Progress, Internet-Draft, draft-reddy-tls-slhdsa-02, 17 November 2025, <https://datatracker.ietf.org/doc/html/draft-reddy-tls-slhdsa-02>.

Author’s Address

Richard Barnes
Cisco
Email: rlb@ipv.sx