

Crypto Forum
Internet-Draft
Intended status: Informational
Expires: 4 September 2025

D. Connolly
SandboxAQ
3 March 2025

SHA-3 for HPKE
draft-connolly-cfrg-sha3-hpke-00

Abstract

This document defines Secure Hashing Algorithm-3 (SHA-3) options for Hybrid Public-Key Encryption (HPKE) as registered KDFs.

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://dconnolly.github.io/draft-connolly-cfrg-sha3-hpke/draft-connolly-cfrg-sha3-hpke.html>. Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-connolly-cfrg-sha3-hpke/>.

Discussion of this document takes place on the Crypto Forum mailing list (<mailto:cfrg@ietf.org>), which is archived at <https://mailarchive.ietf.org/arch/browse/cfrg>. Subscribe at <https://www.ietf.org/mailman/listinfo/cfrg/>.

Source for this draft and an issue tracker can be found at <https://github.com/dconnolly/draft-connolly-cfrg-sha3-hpke>.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 4 September 2025.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Table of Contents

1. Introduction	2
2. Conventions and Definitions	2
3. Security Considerations	2
4. IANA Considerations	2
5. Normative References	3
Acknowledgments	3
Author's Address	3

1. Introduction

TODO Introduction

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. Security Considerations

TODO Security

4. IANA Considerations

This document requests/registers three new entries to the "HPKE KDF Identifiers" registry.

Value: 0x0004 (please) KDF:

SHA3-256 Nh: The output size of the Extract function in bytes

32 Reference:

[FIPS202]

Value: 0x0005 (please) KDF:

SHA3-384 Nh: The output size of the Extract function in bytes

48 Reference:

[FIPS202]

Value: 0x0006 (please) KDF:

SHA3-512 Nh: The output size of the Extract function in bytes

64 Reference:

[FIPS202]

5. Normative References

- [FIPS202] "SHA-3 standard :: permutation-based hash and extendable-output functions", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.202, 2015, <<https://doi.org/10.6028/nist.fips.202>>.
- [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>>.
- [RFC9180] Barnes, R., Bhargavan, K., Lipp, B., and C. Wood, "Hybrid Public Key Encryption", RFC 9180, DOI 10.17487/RFC9180, February 2022, <<https://www.rfc-editor.org/rfc/rfc9180>>.

Acknowledgments

TODO acknowledge.

Author's Address

Deirdre Connolly
SandboxAQ
Email: durumcrustulum@gmail.com