Workgroup: CBOR Object Signing and Encryption
Internet-Draft: draft-ietf-cose-dilithium-02
Published: 12 January 2024
Intended Status: Standards Track
Expires: 15 July 2024
Authors: M. Prorock
mesur.io
O. Steele
Transmute
R. Misoczki
Google
M. Osborne
IBM
C. Cloostermans
NXP

ML-DSA for JOSE and COSE

Abstract

This document describes JOSE and COSE serializations for ML-DSA, which was derived from Dilithium, a Post-Quantum Cryptography (PQC) based digital signature scheme.

This document does not define any new cryptography, only seralizations of existing cryptographic systems described in [FIPS-204].

Note to RFC Editor: This document should not proceed to AUTH48 until NIST completes paramater tuning and selection as a part of the PQC standardization process.

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://cose-wg.github.io/draft-ietf-cose-dilithium/draft-ietf-cose-dilithium.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-cose-dilithium/.

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

Source for this draft and an issue tracker can be found at https://github.com/cose-wg/draft-ietf-cose-dilithium.

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 15 July 2024.

Copyright Notice

Copyright (c) 2024 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. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

ML-DSA is derived from Version 3.1 of CRYSTALS-DILITHIUM, as noted in [FIPS-204].

CRYSTALS-DILITHIUM is one of the post quantum cryptography algorithms selected in [NIST-PQC-2022].

TODO: Add complete examples for ML-DSA-44, ML-DSA-65, ML-DSA-87.

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. The ML-DSA Algorithm Family

The ML-DSA Signature Scheme is paramaterized to support different security level.

This document requests the registration of the following algorithms in [IANA.jose]:

Name	alg	Description
ML-DSA-44	ML-DSA-44	JSON Web Signature Algorithm for ML-DSA-44
ML-DSA-65	ML-DSA-65	JSON Web Signature Algorithm for ML-DSA-65
ML-DSA-87	ML-DSA-87	JSON Web Signature Algorithm for ML-DSA-87

Table 1: JOSE algorithms for ML-DSA

This document requests the registration of the following algorithms in [IANA.cose]:

Name	alg	Description
ML-DSA-44	TBD (requested assignment -48)	CBOR Object Signing Algorithm for ML-DSA-44
ML-DSA-65	TBD (requested assignment -49)	CBOR Object Signing Algorithm for ML-DSA-65
ML-DSA-87	TBD (requested assignment -50)	CBOR Object Signing Algorithm for ML-DSA-87

Table 2: COSE algorithms for ML-DSA

4. The ML-DSA Key Type

Private and Public Keys are produced to enable the sign and verify opertaions for each of the ML-DSA Algorithms.

This document requests the registration of the following key types in [IANA.jose]:

Name	kty	Description
ML-DSA	ML-DSA	JSON Web Key Type for the ML-DSA Algorithm Family.

Table 3: JSON Web Key Type for ML-DSA

This document requests the registration of the following algorithms in [IANA.cose]:

Name	kty	Description
ML-DSA	TBD (requested assignment 7)	COSE Key Type for the ML-DSA Algorithm Family.

Table 4: COSE Key Type for ML-DSA

5. Security Considerations

TODO Security

6. IANA Considerations

6.1. Additions to Existing Registries

6.1.1. New COSE Algorithms

*Name: ML-DSA-44

*Label: TBD (requested assignment -48)

*Value type: int

*Value registry: [IANA.cose]

*Description: CBOR Object Signing Algorithm for ML-DSA-44

*Name: ML-DSA-65

*Label: TBD (requested assignment -49)

*Value type: int

*Value registry: [IANA.cose]

*Description: CBOR Object Signing Algorithm for ML-DSA-65

*Name: ML-DSA-87

*Label: TBD (requested assignment -50)

*Value type: int

*Value registry: [IANA.cose]

*Description: CBOR Object Signing Algorithm for ML-DSA-87

6.1.2. New COSE Key Types

*Name: ML-DSA

*Label: TBD (requested assignment 7)

*Value type: int

*Value registry: [IANA.cose]

*Description: COSE Key Type for the ML-DSA Algorithm Family

6.1.3. New JOSE Algorithms

*Name: ML-DSA-44

*Value registry: [IANA.jose] Algorithms

*Description: JSON Web Signature Algorithm for ML-DSA-44

*Name: ML-DSA-65

*Value registry: [IANA.jose] Algorithms

*Description: JSON Web Signature Algorithm for ML-DSA-65

*Name: ML-DSA-87

*Value registry: [IANA.jose] Algorithms

*Description: JSON Web Signature Algorithm for ML-DSA-87

6.1.4. New JOSE Key Types

*Name: ML-DSA

*Value registry: [IANA.jose] Algorithms

*Description: JSON Web Key Type for the ML-DSA Algorithm Family.

7. References

7.1. Normative References

[IANA.cose] IANA, "CBOR Object Signing and Encryption (COSE)", <http://www.iana.org/assignments/cose>.

[IANA.jose] IANA, "JSON Object Signing and Encryption (JOSE)", <http://www.iana.org/assignments/jose>.

[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>.

7.2. Informative References

[FIPS-204] "Module-Lattice-Based Digital Signature Standard", n.d., <https://csrc.nist.gov/pubs/fips/204/ipd>.

[NIST-PQC-2022] "Selected Algorithms 2022", n.d., <https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022>.

Appendix A. Examples

A.1. JOSE

A.1.1. Key Pair

```
{
  "kty": "ML-DSA",
  "alg": "ML-DSA-44",
  "pub": "V53SIdVF...uvw2nuCQ",
  "priv": "V53SIdVF...cDKLbsBY"
}
```

Figure 1: Example ML-DSA-44 Private JSON Web Key

```
{
  "kty": "ML-DSA",
  "alg": "ML-DSA-44",
  "pub": "V53SIdVF...uvw2nuCQ"
}
```

Figure 2: Example ML-DSA-44 Public JSON Web Key

A.1.2. Thumbprint URI

TODO

A.1.3. JSON Web Signature

```
{
  "alg": "ML-DSA-44"
}
```

Figure 3: Example ML-DSA-44 Decoded Protected Header

```
eyJhbGciOiJ...LCJraWQiOiI0MiJ9\
.\
eyJpc3MiOiJ1cm46d...XVpZDo0NTYifQ\
.\
5MSEgQ0dZB4SeLC...AAAAAABIhMUE
```

Figure 4: Example ML-DSA-44 Compact JSON Web Signature

A.2. COSE

A.2.1. Key Pair

```
{                                 / COSE Key               /
  1: 7,                           / ML-DSA Key Type        /
  3: -48,                         / ML-DSA-44 Algorithm    /
  -13: h'7803c0f9...3f6e2c70',    / ML-DSA Private Key     /
  -14: h'7803c0f9...3bba7abd',    / ML-DSA Public Key      /
}
```

Figure 5: Example ML-DSA-44 Private COSE Key

```
{                                 / COSE Key               /
  1: 7,                           / ML-DSA Key Type        /
  3: -48,                         / ML-DSA-44 Algorithm    /
  -13: h'7803c0f9...3f6e2c70'     / ML-DSA Private Key     /
}
```

Figure 6: Example ML-DSA-44 Public COSE Key

A.2.2. Thumbprint URI

TODO

A.2.3. COSE Sign 1

```
{                                / Protected                /
  1: -48                         / Algorithm                /
}
```

Figure 7: Example ML-DSA-44 COSE Protected Header

```
18(                                / COSE Sign 1             /
    [
      h'a10139d902',               / Protected               /
      {},                          / Unprotected             /
      h'66616b65',                 / Payload                 /
      h'53e855e8...0f263549'       / Signature               /
    ]
)
```

Figure 8: Example ML-DSA-44 COSE Sign 1

Acknowledgments

TODO acknowledge.

Authors' Addresses

Michael Prorock
mesur.io

Email: mprorock@mesur.io

Orie Steele
Transmute

Email: orie@transmute.industries

Rafael Misoczki
Google

Email: rafaelmisoczki@google.com

Michael Osborne
IBM

Email: osb@zurich.ibm.com

Christine Cloostermans
NXP

Email: christine.cloostermans@nxp.com