CBOR Object Signing and Encryption
Internet-Draft
Intended status: Standards Track
Expires: 15 April 2026

M. Prorock
mesur.io
O. Steele
Tradeverifyd
H. Tschofenig
H-BRS

12 October 2025

SLH-DSA for JOSE and COSE
draft-ietf-cose-sphincs-plus-06

Abstract

This document specifies JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE) serializations for Stateless Hash-Based Digital Signature Standard (SLH-DSA), a Post-Quantum Cryptography (PQC) digital signature scheme defined in US NIST FIPS 205.

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-sphincs-plus/draft-ietf-cose-sphincs-plus.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-cose-sphincs-plus/.

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-sphincs-plus.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document specifies JSON Object Signing and Encryption (JOSE) [RFC7515] and CBOR Object Signing and Encryption (COSE) [RFC9052] serializations for the Stateless Hash-Based Digital Signature Standard (SLH-DSA), which was derived from Version 3.1 of SPHINCS+, a Post-Quantum Cryptography (PQC) based digital signature scheme standardized in [FIPS-205].

This document builds on the Algorithm Key Pair (AKP) type, as defined in [I-D.ietf-cose-dilithium]. The AKP type enables flexible representation of keys used across different post-quantum cryptographic algorithms, including SLH-DSA.

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 SLH-DSA Algorithm Family

The SLH-DSA Signature Scheme is parameterized to support different security levels.

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

Name	alg	Description
SLH-DSA-SHA2-128s	SLH-DSA-SHA2-128s	JSON Web Signature Algorithm for SLH-DSA-SHA2-128s
SLH-DSA-SHAKE-128s	SLH-DSA-SHAKE-128s	JSON Web Signature Algorithm for SLH-DSA-SHAKE-128s
SLH-DSA-SHA2-128f	SLH-DSA-SHA2-128f	JSON Web Signature Algorithm for SLH-DSA-SHA2-128f

Table 1: JOSE Algorithms for SLH-DSA

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

Name	alg	Description
SLH-DSA-SHA2-128s	TBD1 (-51)	CBOR Object Signing Algorithm for SLH-DSA-SHA2-128s
SLH-DSA-SHAKE-128s	TBD2 (-52)	CBOR Object Signing Algorithm for SLH-DSA-SHAKE-128s
SLH-DSA-SHA2-128f	TBD3 (-53)	CBOR Object Signing Algorithm for SLH-DSA-SHA2-128f

Table 2: COSE Algorithms for SLH-DSA

4. SLH-DSA Keys

Private and public keys are produced to enable the sign and verify operations for each of the SLH-DSA algorithms.

The SLH-DSA Algorithm Family uses the Algorithm Key Pair (AKP) key type, as defined in [I-D.ietf-cose-dilithium]. This ensures compatibility across different cryptographic algorithms that use AKP for key representation.

The specific algorithms for SLH-DSA, such as SLH-DSA-SHA2-128s, SLH-DSA-SHAKE-128s, and SLH-DSA-SHA2-128f, are defined in this document and are used in the alg value of an AKP key representation to specify the corresponding algorithm.

Thumbprints for SLH-DSA keys are computed according to the process described in [I-D.ietf-cose-dilithium].

5. Security Considerations

The security considerations of [RFC7515], [RFC7517] and [RFC9053] apply to this specification as well.

A detailed security analysis of SLH-DSA is beyond the scope of this specification; see [FIPS-205] for additional details.

The following considerations apply to all parameter sets described in this specification.

5.1. Validating Public Keys

All algorithms that operate on public keys require validation before use. For sign, verify and proof schemes, the use of KeyValidate is REQUIRED.

5.2. Side-Channel Attacks

Implementations of the signing algorithm SHOULD protect the secret key from side-channel attacks. Any implementation of SLH-DSA signing algorithms SHOULD employ at least the following best practices:

* Constant-time operation

* Consistent instruction sequence and memory access

* Uniform sampling without information leakage

5.3. Randomness considerations

All nonces MUST originate from a trusted and cryptographically secure source of randomness.

6. IANA Considerations

6.1. New COSE Algorithms

IANA is requested to add the following entries to the COSE Algorithms Registry.

The following registration templates are provided in accordance with the procedures described in [RFC9053] and [RFC9054].

6.1.1. SLH-DSA-SHA2-128s

* Name: SLH-DSA-SHA2-128s
* Value: TBD1 (requested assignment -51)
* Description: CBOR Object Signing Algorithm for SLH-DSA-SHA2-128s
* Capabilities: [kty]
* Change Controller: IETF
* Reference: RFC XXXX
* Recommended: Yes

6.1.2. SLH-DSA-SHAKE-128s

* Name: SLH-DSA-SHAKE-128s
* Value: TBD2 (requested assignment -52)
* Description: CBOR Object Signing Algorithm for SLH-DSA-SHAKE-128s
* Capabilities: [kty]
* Change Controller: IETF
* Reference: RFC XXXX
* Recommended: Yes

6.1.3. SLH-DSA-SHA2-128f

* Name: SLH-DSA-SHA2-128f
* Value: TBD3 (requested assignment -53)
* Description: CBOR Object Signing Algorithm for SLH-DSA-SHA2-128f
* Capabilities: [kty]
* Change Controller: IETF
* Reference: RFC XXXX

* Recommended: Yes

6.2. New JOSE Algorithms

IANA is requested to add the following entries to the JSON Web Signature and Encryption Algorithms Registry.

The following completed registration templates are provided as described in [RFC7518].

6.2.1. SLH-DSA-SHA2-128s

* Algorithm Name: SLH-DSA-SHA2-128s
* Algorithm Description: SLH-DSA-SHA2-128s as described in FIPS 205.
* Algorithm Usage Location(s): alg
* JOSE Implementation Requirements: Optional
* Change Controller: IETF
* Specification Document(s): RFC XXXX
* Algorithm Analysis Documents(s): [FIPS-205]

6.2.2. SLH-DSA-SHAKE-128s

* Algorithm Name: SLH-DSA-SHAKE-128s
* Algorithm Description: SLH-DSA-SHAKE-128s as described in FIPS 205.
* Algorithm Usage Location(s): alg
* JOSE Implementation Requirements: Optional
* Change Controller: IETF
* Specification Document(s): RFC XXXX
* Algorithm Analysis Documents(s): [FIPS-205]

6.2.3. SLH-DSA-SHA2-128f

* Algorithm Name: SLH-DSA-SHA2-128f
* Algorithm Description: SLH-DSA-SHA2-128f as described in FIPS 205.

* Algorithm Usage Location(s): alg

* JOSE Implementation Requirements: Optional

* Change Controller: IETF

* Specification Document(s): RFC XXXX

* Algorithm Analysis Documents(s): [FIPS-205]

7. References

7.1. Normative References

[FIPS-205] "Stateless Hash-Based Digital Signature Standard", n.d., <https://doi.org/10.6028/NIST.FIPS.205>.

[I-D.ietf-cose-dilithium] Prorock, M. and O. Steele, "ML-DSA for JOSE and COSE", Work in Progress, Internet-Draft, draft-ietf-cose-dilithium-09, 12 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-dilithium-09>.

[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>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/rfc/rfc7515>.

[RFC7517] Jones, M., "JSON Web Key (JWK)", RFC 7517, DOI 10.17487/RFC7517, May 2015, <https://www.rfc-editor.org/rfc/rfc7517>.

[RFC7518] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518, May 2015, <https://www.rfc-editor.org/rfc/rfc7518>.

[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>.

[RFC9052] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <https://www.rfc-editor.org/rfc/rfc9052>.

[RFC9053] Schaad, J., "CBOR Object Signing and Encryption (COSE): Initial Algorithms", RFC 9053, DOI 10.17487/RFC9053, August 2022, <https://www.rfc-editor.org/rfc/rfc9053>.

[RFC9054] Schaad, J., "CBOR Object Signing and Encryption (COSE): Hash Algorithms", RFC 9054, DOI 10.17487/RFC9054, August 2022, <https://www.rfc-editor.org/rfc/rfc9054>.

7.2. Informative References

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

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

Appendix A. Examples

A.1. JOSE

A.1.1. Key Pair

```
{
  "kty": "AKP",
  "alg": "SLH-DSA-SHA2-128s",
  "pub": "V53SIdVF...uvw2nuCQ",
  "priv": "V53SIdVF...cDKLbsBY"
}
```

Figure 1: Example SLH-DSA-SHA2-128s Private JSON Web Key

```
{
  "kty": "AKP",
  "alg": "SLH-DSA-SHA2-128s",
  "pub": "V53SIdVF...uvw2nuCQ"
}
```

Figure 2: Example SLH-DSA-SHA2-128s Public JSON Web Key

A.1.2. JSON Web Signature

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

Figure 3: Example SLH-DSA-SHA2-128s Compact JSON Web Signature

A.2. COSE

A.2.1. Key Pair

```
{
  1: 7,
  3: -51,
  -1: h'7803c0f9...3f6e2c70',
  -2: h'7803c0f9...3bba7abd'
}
```

Figure 4: Example SLH-DSA-SHA2-128s Private COSE Key

```
{
  1: 7,
  3: -51,
  -2: h'7803c0f9...3bba7abd'
}
```

Figure 5: Example SLH-DSA-SHA2-128s Public COSE Key

A.2.2. COSE_Sign1 Example

```
18([
  <<{1: -51}>>,
  {},
  h'66616b65',
  h'53e855e8...0f263549'
])
```

Figure 6: Example SLH-DSA-SHA2-128s COSE Sign1

Acknowledgments

We would like to thank Roy Williams, Cedric Fournet, Simo Sorce, Ilari Liusvaara, Neil Madden, Anders Rundgren, David Waite, and Russ Housley for their review feedback.

Contributors

Rafael Misoczki
Google
Email: rafaelmisoczki@google.com

Michael Osborne
IBM
Email: osb@zurich.ibm.com

Christine Cloostermans
NXP
Email: christine.cloostermans@nxp.com

Authors' Addresses

Michael Prorock
mesur.io
Email: mprorock@mesur.io

Orie Steele
Tradeverifyd
Email: orie@or13.io

Hannes Tschofenig
University of Applied Sciences Bonn-Rhein-Sieg
Germany
Email: hannes.tschofenig@gmx.net