CBOR Object Signing and Encryption
Internet-Draft
Intended status: Standards Track
Expires: 16 September 2026

M. Prorock
mesur.io
O. Steele
Tradeverifyd
H. Tschofenig
UniBw M.

15 March 2026

SLH-DSA for JOSE and COSE
draft-ietf-cose-sphincs-plus-07

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. Pre-Hash and Hashing Considerations

SLH-DSA, as specified in [FIPS-205], supports both pure and pre-hash modes. This document specifies only the pure mode of SLH-DSA for use with JOSE and COSE.

This document does not define or register separate HashSLH-DSA algorithm identifiers for JOSE or COSE. Doing so would require distinct algorithm registrations and would introduce additional implementation and interoperability complexity. The algorithm identifiers defined in this document therefore refer only to the pure SLH-DSA variants.

For many COSE use cases, this restriction is acceptable because the application can already structure the signed content in a way that limits the amount of data processed directly by the signature algorithm. In particular, applications that need to sign large payloads, detached content, or remotely held content may use the COSE Hash Envelope mechanism [I-D.ietf-cose-hash-envelope].

Hash Envelope can provide operational properties similar to those sought from a pre-hash signature mode, such as reduced data transfer to a signer, reduced buffering requirements, and simplified remote-signing workflows. However, Hash Envelope is not cryptographically identical to a standardized pre-hash variant of SLH-DSA. In Hash Envelope, a digest is carried and signed at the COSE layer, whereas in a pre-hash signature algorithm the hashing step is part of the algorithm definition itself.

Applications that use Hash Envelope together with SLH-DSA need to ensure that the digest is recomputed over the original content and compared with the signed digest before treating the signature as valid for that content. Profiles that rely on this construction SHOULD specify the permitted hash algorithms and the verification procedure explicitly.

If future deployment experience shows clear demand for algorithm-level pre-hash semantics in JOSE or COSE, separate registrations for HashSLH-DSA could be defined in a future specification.

5.2. 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.

5.3. 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

5.4. 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-11, 15 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-dilithium-11>.

[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

[I-D.ietf-cose-hash-envelope]
Steele, O., Lasker, S., and H. Birkholz, "COSE Hash Envelope", Work in Progress, Internet-Draft, draft-ietf-cose-hash-envelope-10, 15 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-hash-envelope-10>.

[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

```
{
  / kty AKP                / 1: 7,
  / alg SLH-DSA-SHA2-128s  / 3: -51,
  / kid                    / 2: h'736c682d6473612d313238732d6b6964',
  / public key             / -1:
h'f3eb7b23659086bd1d5196f8201898c189ae9fd5567be8941f135e54b261ca9d',
  / private key            / -2:
h'4d9884c45556898d0da29c5af418386d9abcdb84426e64ab44e5bcb3126c77de
  f3eb7b23659086bd1d5196f8201898c189ae9fd5567be8941f135e54b261ca9d'
}
```

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

A.2.2. COSE Sign1

```
18([
  <<{
    / alg SLH-DSA-SHA2-128s / 1: -51,
  }>>,
  / unprotected / {},
  / payload / h'66616b65',
  / signature /
h'66f177b396bbcb70fd813db15c6805d80c921ca441ff22c7f274c7e7309741de
  407015cb0f4b60cbb585dea1ac00b5807d6b2e8b5c3b2cb8cd52b37f9859c96b
  13cedf81cb33971578165adae61852b5665e02a36701bcf55ed24858ed039c83
  a0ccb6ec3066efd7523388a8f7753345159371af2ad5e5af15274d4ef8d74c5c
  5aea8a289fe96a5fc351383e1e4bcde1e807d7a5bf30a01e9713ffbca9065ff8
  f10d27ad1e3986d6db5eca74356d1bca6b99d3e278f6f605cb0decdaa9c4903d
  b15bbe9bd7899836de452f26b27f41f3e0a8d75cc3d00a7e0ad4fe9ddc177ff3
  40b9871a68092fab794463d7ad99ca75f3570cc9f37d9147542e0313ce4d357c
  7cd4fc7769db66c7d409752276530a8e35080747859eb70e26d5e25200db1197
  28b3e5f0618ff7769f5f3db564a08f0f82705fbbbeed16dda86d0ce5e38da3c3
  e595ef7c7d9fa217ddccc5f2443f9602bb4b27735c107426659f9437b16db32f
  01b6b804de051964001f31d653f62e3241cc45f16a78ffd14ff192a1dccaf4f7
  1522295ec4da6fa872d9fcfe2cb25f2d239f4fc1b223293d00f57a03f005a9fd
  73f5c00a68a47b14c0f24f118a523f6cade374a33c151e328f20cb8762e4e28f
```

```
1bc80a2c98da2a78fc1c11b5531b119fedd55b64992c9fb47195b91ee02cdc9e
8e354091dfbf3846e24e162077d152772cb2abeda9e848ea015fc936fc4acea0
867dae7f1294cb947845ff8b3fe695d8b0857b5085ed66dbc381c56772f810f4
01ac1e852284004de398cc2ef996d6db3538c822298579bfd856da9502e8dabb
c912a4438ff6a031d26f28626d0a0576ffd60dc2dc59a5ff9978569c8590fd93
1f8e51c0d63165a1640daca84f496c0c7121692ff141b40e64ddf002b8d36353
cef6e4a07a7afdb2f799d856a1197facc02b5aa8b323ef8748a5702dc7d9056e
63979eecac1d4e24a8d8c6b059460a626f2acbe0623027dc6dbcb7330f1ceb65
4ec96f6ef123f0c56c1c997d0298024ac2a6a754d7931386e168020cf8f53929
4037deacd6c63accce54657cd26603ad74f5231a2298805c0e555b67f11ccf8c
af4aa69fd59778175e01d992d77f10fe76668f2ebaaef5448a75ecfb740ec0c2
52ef40b758d54874473fe1d4f2ff3bb3c5d64c095354d23d04c6147caf7f48bc
b593851d7708d4188d370570a17abc765346ce6b1d578d5d883ba0c7d3fc2711
483fbc94df2e3954c2303a63f9bdde91321489dffdec39202b7fffe12f5ece45
2ef0900580df8bfc1a763a0f6add1b318a9e9c23223e20ff0f793bcdff065756
7c6de15b98c947b6f9228cbce87d0437ab992384a7210c17de265914423bf07b
795d3200c80eb5df56d9a69d01cf554030e9e779832f65e0b3007f0c59fd1e97
c368c47ef83245cbf0ef3f2a26ad22f7e640c398d6c39984df506b7f8f4b6042
b9a8fd419c238cc1340b4013763958bf7584a6bad7ae87610aa15b53198236e7
57ed72bc231877322a80b007ae6806d7339151842a6ce78bc1b180de8b7d38b0
0b1f56b831e7fc4de78a887f375547ff78bad535a9ce4c12491ce46d80dc72f6
c1eaac4e5f53e52c9139151bda2641417e1ebeb41482d23fd0dacedea8fdd0cd
11e371cd540e141c8f07820478979a65743ae27e49b59645de0f5b7f53bf4030
6da8a3a33208c79910f795f81edb5688d06f5cf2554301d3ddc0b67318201f2d
33086188ff467f11f57f343c51f889b4db07dff945de937e6eb481ae8dd7217a
6572bb245b5b609b39431457947d0d054dc778c8c48279bdf6a39dcff80ff2fc
53792438355f051bb64c1e1d6c44160239ee702460052e9462b61fe5f5d26523
ebf89541b6f02ae622edf77487a2b527326fe106b6e9f9e32460855e55761186
dd1ab3bc9d23d8c7c362a0162182e717081f9a469f078e844a4bfd86b5d4d21c
a40153c20b72b781e9f62feb373bd46de710bdd6de1c48b235092b0945788a14
6d6a4638e09c5129a32ae13ed4156fb3196cbec6a6e1992d363de1b21635619d
d1591875e456c7cd8437af0b919f6021a88bc141f862d7c97c84341ceef8a75d
a56906d9668c7dd177177d42f53337a3e1689e2cccf618523160fe54940b7947
68124642d830dbb8fe13b4c6294468e57405f68e06c78ebe32d265124d6ffd25
8853c5266cacb9022150d20b12fa5731e9a1aface2ee8ba1c3c03caf91b84098
d84db5268c54968414b506bb514daafaec44450ac095f6d56e0f3b29626eea46
883145762973eb7b75e219c8875e4f2f713f3bb400209ad342faadce742fea8a
264913c7e4c04062bf7f07cc9ddf030733e2badf3e3bc7d6595a3142830051c0
21bf95476a6d49e0237ac500158ce6913077c7f56ce5980bb896c3e40bad0e61
872b4e5fa8bcabb0764f49b5ebc5b2b4da0d909889845e9187336b9e67495c3b
6794a0a7268c60f1d884f13e4db78d37e43f2ad05ab3fa9dbe95d637596a87d3
8aa69fe1da45c8e45f0405a5c8f6922430a301287a2c58bc38cf46b5fa07724c
18d973f554f87fef904e942f63029a5a0ef01b57744d71c50ae07225a0bce392
0fd74a2fede6d9613b808f52720224871518dcf848a386e324f52c13229743ca
70574f0dedb6c6b9354370f4a6aeb172b145c49e1160ede3b4ace912a8d98993
f15212626a8d7be8c9455fee7b2cd30a4153638dc08f08853789026057d4d38f
70352d73a40feffdf7b5adb01217929628d97171915e913441d244dcf8c88496
256fd75c7ec5f0686cd02c41ea12f972147db3b330439b8d15641bfa6432f01a
```

```
d832251ae6b5fca6079fc8ec68adc0a96589a57b8b27dfdf79fb717f4729dcf0
399cd92f2967805cb7932df9dcbc21fedc0700c6abf099b7089cf79cbc80210d
9da725e65094ed87509250ae6e3970cdc9ca04d783a3bcbddd15cf0f7026efff
cf23b8894081dc7f12a62a44be91b2e587612c025d53ff90060abd242f364da8
6d404f2c9be397de8c666b931550222588b881fad8ce8ba1460a5f469fd8672b
086d0d233e09ead31ba11907dcec6db0a9b5c1aff5e527cdaa1a494fc8f45545
ff711b464a35b3dfe8a1a1749b27778f52aaefd623c24be16810ce18d8109c7d
69bd9fa8a766cfc05fe33befbdc2cd5cfbc2f817e675574ba0fded4b0a4f1c9a
700ec5a39e5b7c6a3beff58934d5e715e376e5744ded919cd2a1be9ae52a2cfa
cf85b7138efaa7d88bc6113438f462dbbce231e872b6804aa755e9bdc7c7f232
e52737a508805b5c5e19ebe3c5d61e6edfe06d1e5be75c3e56baa7b5f2be7fbe
064290070d0fb23dc64fd35ef7ab92ffa8e894e9aa709b9629619ebd12008fac
91bb3b29ad584e4d0fe0423641601e1256460e13da6b42a68df876b1eac22572
f5d77cce23589630e86861a6ec7048dc70263cf04baaa92b3c80a444df3c5edf
d093a3a9a59ae2bd6add4e944a022e2c8f1f75dede0544d8fca90e32b79142eb
87ecd146976d301a4c77b623f3adbd3a1f8776821695a9233e2931048484e357
0da59dff1da8f2a1f6e1186f84615668c823d5ae08727a613e7e1f946a5da202
afb848067c9d45a5002f4724e7ac0d163fbe583163ce48e5cb2adcd26f4ec96a
498dfa4871788b6273f5cabd27eeb5df9249ef09b530a25e7e87296068023ab0
edd9a2039ee9ee3a7129469aaded974163c1f56d373f3c420d5e4aa9d504ecbb
116ff639fa90a968c9d85b8cea6ac9e96be7edf9c9c4ab733c619aa91017571f
de4f3fe509c3542b4b5b65989a8dea001bd91a3ed64eb9ac0772715af0ed3a07
8992a85e5b0137fb90309f5b678a677d8978f408038e28cfa256fa92a47cc753
5e47a01636425b532527e011a6e2a30a62c266cf34a9048b318fbc1831b72c78
ab944398e8516482d13e9eb12ce4044072ef673cb4ec1a316ecb7297dcb4d3d1
3ca3c023f6b57f7c14bdce78fc0f448551296039cd01ff43c05615d87eeca3fa
94bbf3d5a14a99bd109d24914e32ee2aa39eb7f07725767c1ce0c44cf8049904
16a5c009385b99b887b18848fdaa6b53741f9c874adbb957906e531fc194160a
7478b33bc767b2644ef752617cd8bc74a278e92e3996fe2fecefadf2c0c6cfb2
abec03f3e4c2631ec2614c6214835b39f5765abb1ed904a9d2b9d1306e505037
57885f77ffef271a9f4aa537cc84e43a45c898eea806c6e1e1d5bd2051cb7da3
e6a56ac32e77802dd54b389f5d63b2915a1adcf814bd3cde7d8a0d60cf2e8099
f3db0797653e6252f79e23c1678631c560f4db292ddff18d0b916562ca191b29
d502d679b7a6a3fbc6cde479fddfb72f8df707ec8570f3a88ca72f85f72c9516
65669967629207e37c8628ca3faa6a826febbadba9756880353dc7687fbfb19a
249e4ca33d1be672399134a6618fb511e8fcb04deae7317eb9e312f61a569030
ba703e027712d11d14b5c76a1c7d2ae03af18ffd9eb02fcc956353bc03d934dd
58050b798c2765393c531121214e0db4e65977c2c2f7263028a08befef29b902
f44b073a27a480f22f8f1e1632bbdaac20b480478f0cb2c200556f1aa969d16a
78e38a17e8cc25141be118425d71355a647dfd727b138a906530fd0412d247fa
7faea2b839fe104d9997f1c4b53398a12f41e305cd91d60ae0468510f52326b9
cafd32275cdef7b6a0c5d01ef2617c5c9081f56863377dcc62382ccd54f7eb7a
b29b1dc8f73441f761e4fe1ac184fbe90067d506f93d602764a75545002d2f57
2e0dd66219ab8b8099417d6dc35a5fb003e1b6e6991385ecfd857be8b28d5621
476485116e1ca1d5885137ea2da6bc0488e6a17fc3d5ee09af187dc3fb044d57
fe9447a8a2ecc825d24d2a023fed1236059d6be8a73e4476440c7040b8d27bc8
43781148b60e2add903b5a49a5599e6d3f60cf00cd6f915cde8153b193d1094c
77a8e20bfe6c165f62c7bc6bd7a21a009c2d412c0f466ec668e3a2ae92e90ae6
```

```
d63e7d18943b28991c4fac002c30dd982bac2aa0df59775b03a9ad9982d494ed
0c78872819257853b2c9459e4fa3ff0000f26abef4e9b850ba51f7e9bd4c9d04
24832d1f3e73b24fe27a95b54c043b1bb56a9f3ee60b62ebbccb159bc0e3b085
23525026eb5bddad94d02315075fa8214ec930c9c95b26abbbbca5b5cda2a893
8ffadb3f68c97d543a8547a7eb58d899889397abedf2971c95f05fff8cf5269f
6369923c51885ee22dcacfa6ac0eaa7416ab774482cf156dbd5c6dbd1993d83a
6b4b35d60e146c451acbab7bcc1896b31430aa5c57ceaac1ab8ef8abdf73f6c6
b18e649e0f81f051791388eb06ac907024d44bf5db8db3a2fd2e73df759c519c
5d7f2ba3db057d6692467603aaa895cf32b44157ec0932951d3d3d6e33d2509d
089944fc160d51cf70b14c70533714efe9f0607d2746f72296991b2fe8906982
e4b08a524a163eb3cd5f8e5a571cfeeb2e2791bb0932c85f224c170a0eace43c
e98f993ec8ab446a3150a8152dd8bb6f52acfb8674df2104c705fe48c788c167
fe353f4872f87fc27ae7c6a13bdcc8545a8f696d04c56564f7d2db2cbb2e7f20
9a2e36407eca21fcc792f170d7696828f7217927585030e6455d41de5e8f0232
55659f0c1e13b3b088957882f0a2a791474b87160275bcb42b086f0882d9b580
a210932b69d63d34452303c98b93f9474423fbd06c96f4769194261ac9564750
e9cb081a3a4363d15392994ef57179b46908a31e0a0adf472596fac729cf5bd1
0f566d1c8458e9ae6aa921c7cb44153476c4bbd23f0cb62fd30139692c6b925b
a3c7f09d2de4c116d18f133dc1cac6dca05eb3ed019e585d755b55784f6c9b91
bfe074092ad18e42e802d0ae43eab5c0daeba319407ba7612ab2f819b74e8242
c5dc087eb63307491212344cb1758c0a0be49aacacae24501f0dccdefbfe47a3
cf2f57e8023826caf01e46f8dc57e79c8782b5da54186363db57442da7e9f8d1
5396d02ed335dd823e5f403225c4aeccc4e7b5d7cd187e9307fe92f65ab9e7c3
1ed39a9e3a88d6efa4ef8dccbf91c46fbc20d5fc184c54602cb1bde2144d1631
cbb038d2bdd1d01de7cda1ac2d2fc1226a05b029dce23a7d224f0c556bdbaebd
4cbb8e83249db6b0540df78c2951307c12c7b29ee2a07cd8962926241f0c193a
010aa4c8aa5a5bf8187bb20e9a579ddf5bac5c81398f43922dcc65a777a27cf5
60249146b6ea301b76f03c4672b1f9e037082b908b067455495d69f0f636869f
b98bcf71b91b1192f71be9c1b4580ec3b518c83858b4e7f3a8cdbd8e43cd6502
7927a1e051e2498d1c6803d8dc563b7e478223b3046fbae1dceafaecec134fa6
222d08b4fe736274e4d3b00da8be2b5af26badcf64e3beebb77c33e634c700c9
ff9ce0d8b2dca4448c4c32c502d60af3d40826b9f52eff8cf7d86aad35ef662f
5d8b8660b9617efa97cfdb2987f155336257a82939b536e791ec85020eb0f074
6caff8159e047b1bd03524777008e6590c9be41c97b07f9b5f00117200c73643
c7a06096215a0f9a25b0e618cfa8ee123fb1b10f1049305bcfa623a24db0bf51
d0332d73c015ef3bd6709b6ca6e483f50e913f541e264a89b3f08457d3911e01
73a20ee97907ff462e6b84fae1547dda3a47f0787d49f5e7b3bb0570193060cb
0d3fda02213f8afbda3a4052f443e1aef5d790a5196538031ceda5813fa73c05
afaa4ef7b9b5009022ef86d17dc97d33db07bbc2d35e7cc4e725f9a986e1d8b8
fd435e162560b3e72f355a987a0ccd5186c3f8a7d6f7e662526cd63c3112315a
7bb3075521b3a6cc1548878f26638ebac7f57c13b46aeca8ed4f9c81e1b6b8bc
9889388264c8fff31c30ba03aefb4911f20afe58ce657166c0f857f7169f7da8
ffa3ba7bd172bdbb473860eca50836fc105b9ccfe749f453727b7b42cd392396
181223eb3f04936a34375a243ed1620acbd181f949f705e8984df934f1ed09c2
251c6233caa15e39a97a7e52ac8b80be9b8c42ab86fcda5417b913d47a11fa51
ec68d33726436f70718c1062cff5842e117b1700c81617c1fd707988466677fa
c9eef7b6ed424c3c0258cc40e1f95d80ce4724b199ef14aa96545046cd3b3cb1
2cd3b83baf28f7aeb31cfcd3223701eb398938eac7605a8730ca8156e1d7e842
```

```
9a1fe92e50a4f621ee8d709dd8ef8f05ecc66990d9e70ae020d2367cb372780a
fb2ebcb25f2465f1ce77cad0bd10a3a04900be0d59894e4b4d30bec3b6075e67
61c29b87ec4d3f6d8ccc6e610d1bab2a2ebad200f13f9f35bb34a26b410fa0bf
d36262cf3bda7aa7c6b87dd2afa36cc6aaa37648492e4d0a8df1f7192edb6d0b
a76f7114c9e24322f4f4935b9d94214661fe842e07b3136235fb30fd7de9e5b4
ac06f8dc9b3ffa1bde74770f1e46973644736a94d9c6964ad944f3b61e5cc49e
71a775f82f68dbf13b90039c8a53b01092aac77778f7c659c2bfa7e65b1ff68b
e2bc0d47ad3501253623572508 1e38458cc872498c5500cbfe545e7f1bdd2fb9
e467418fbc6c418ad80139eeb737e1550b5cb356aecef14673c2513638b62839
83fcadc857db15f64b75ce832ed0d4aae633aa6cf86808f01420ac141c51d659
e25d335e4d2ba2d23a11dbc974c039f9d26a3bdab5dfef411f97282e26e76ed6
0febb37826dec8ae45580dbd9fbdfdf035eb8e0722b2734975459244c5afcc9c
6ac19e68b97e4b963e1b043cb942481761703a2e88e00d499a67d8d05ce138ba
d64e6237f72846717cce90cce81686ade41eca97d256f10155e23a306479c81d
d43a5acfbb9a6cc4dfa3055a0ade76b46ad92faf1f30c85538f4d651600d07d1
95c8829638d89c0810881bfca46c6bc4d49107daa3e634a18e7f88dbc1035a5b
85f819bb8703df5a437df880fbd37696beee2688eb9dd2f579ff8d32f57fc157
abad5eb6e2ae3ac578943c98a393e3d781e6314770f6f768b334a42aa6614313
94962260208701caa1ba4e4d5e84657d7dbe33b05dd4633315988bf64c52feda
65933d08cd2a42e1eedd3ac48d5f7a0df7a1613c5186a5438e938955b167801d
6fe6770c383530c16ee6157503432ff6d4e8365ccb18250d2f7479a37bca6953
259f26aa12d8c403c1d9173325a29cf2d03e43783405ed4ab975ad6ed1c7efae
c61229c00dbcaf7b444eaef876c7ebebd0744ea317699f7505eb877fce533e6e
3b8efb75888658cc486c60785820aa85afcdcdc7e5dfc5b4c07eb7fe4aedaf52
19fc383f321bbaeb387b26d8f2c1358d69ae980fe2dfa926c73292442279cf61
eba163ccc1cab6c7aca1107d6bfc6c3fae69f1bf785a223828d49d81bfd0d976
6c2504d902aad81c108ed1935feb6df3a0c0c9c18ca30f25c3af61b166f0d591
19d7a678999d4bc8b52094c85d9a1efbbba6d3e80250ee70ce67c301dcd01af9
8c25aeefb65f91eb98bba590933685b71453c771df9d2b56e7785f22c3651ff3
23b4e8ea6fc0e0956907cb227dd53e5941c073d374a0ff0e773c67fac96cd4b9
1af199eada74f143080bd14dc7a6c883e6d4877592bcb9981b9856ad28358442
9deb4a03597adef8b811cb2b70e9acf5a3433653b6e7666489676d759b8aa9e3
32978f9340a7dab0f1115a49554eb1865838848244121b0feffbb9b8756a55c1
85c2e16785b93a4ac997a79a697098769351cf3a11c2ba635d2a20c8cf728259
45b2bf7b97ec661edf65d469783a7c4217c1accc76b9f44e3ffd02f4b628d31e
1ace48eebe2f17f59e069de3634a5859b2c8395c896c6528f35ef1b8ebc41c54
d92783b9b1403e5c3ae8d62b5c907fcd18099eb40deb3a4c17aad15f00cfbd42
92975657038de63a5e5b512a5de85b15de6269eadb0428710de16e70a2ac1e96
c029d07173b03452df3811a18373a13e281291adba0ba77113a0e19488df7144
e7ad56392657e7f03a14aeefca4db09a40ad9157398da9212a6a368202ac1d69
a4e55eac657e0cec4c7ddd6842c8cec9f58d234fbfe9105ca957cc00c9d45269
a3c369826da8de5072f10047a47e2d696bd10499f56f562e9f0f1a7517061132
36be3d0ddfbefc070dfe27527f0da753b032c84f14ef2ef9e3b4f1d1b9af3c3f
0f77e45ce1da34a8584569d2c3567c18afa34420665cc4de19bc8f5a217ff1b0
463a1a84d1e9daad11429ce9495836bfe6b6c715597a0eda74433bdcad336020
70799d85e668aac9cd2122e141bab3640d7dfc786320a0cf4c1ff21b36f4405f
c563083a0d9a90c345b7945e258d615808232ec765817547f73684adbfe3f669
ec7b88c0a2a3ad3eab8ef069fa6c0d9539428c05f69983d9d9e35a2773fe2ebf
```

```
    677d1eba73bc7e877ec6f0f19c6b6b821b9666a4411f04b795cb0cd88d94bf06
    6fdc92c94fe1bdea31e0fcccfc7a7f2280601756f043a2442d7e694c245e572f
    46f154195189ec29a868557ae1681cfa56abf2d97300a26fb23874e86365c9ea
    ad15f7d123f4bb55f018e818ff54df664e37d019847827239145e82bceff32e0
    c2141c15ec80b3a7305642897926d1baf7f60b121e773cc490030fc419a0af46
    65e1deb293368a525f9fb9a1fecf996183da16bb79b97c2b2947192ab5c2e61d
    88198e9e11bfb987788f272b5dd5904e15f63b5534a5505e0c21abc281a6eff3
    9cd20b7e361e591b949f751a0f350eb093efa2256ea210c573d38ab5a06bec62
    0236efe6eb32df9ca4bb67c21c7a8eb7c43dd90a4d467776fb47cf23c4d09d2b
    193d3149b6f3256c3edfcf1171feef5a980446a8658a4e952c3edd6b7fd08b01
    a4f547307fe031be36e2014c36e98d7c8ae0b40d935fbc68db4cf809232a48df
    dbc813997a42a7e2c8ad19d3568f6d156bba42a911fa85cd59b9b4ff44d94e59
    5d7b22e416dbcb987464f60e7bfa4187a1f7689bbbcb36398e51bcd6900a8655
    50c3a2e35343ac75cf07e016db8379e4ee68c71e57d86bbb68b97c33f03f8fec
    786d8cedbc51588ffe92e4a330871b331352b7bfe751f148214c76f39f6f2c4d
    ecea95c1a4c9c22d79f1bd0196f347756440ed051398d5bb46bcb5561d2d41fb
    0c9b2ea07af138d98dcb9e268cb95fee1dc02b2feb11967a255185bc96c2593b
    7e350f9d3ddc4bf2b073061a1eba3667f84a198a05203121108dddc0c84740b6
    53dc8ecdf99d40f68446342836cd24de0bb9f4558056fa60a5f1eac5a1f3bda9
    2b0b2a03812efa05dc3482d44ff136e425d2e42a6b260513266d25fed20128bd
    3e6b67a63f1c2920939bfca85c365b07b47efeaca3955f89ab18474e4828e611
    3dcba968d2080f978616ab99f378b591bb15f0c1b6a8b7a2a59acb5fe5db0b77
    d9935de09bbcdbbb066b77ac114548cfd4399a4d2c480b4d324c2bf9b11d23d5
    33b1ad32bbf85d952596caa6af7896ade2c17e18da88bb044be702f221a9505b
    f9419f725ae0ef030b3c89c3b043397184553a5e431231aa9994b38e85c03800
    49a6f711777c70e3bbeeb264571c890f983bf39565b16f667afd881a8c49c589
    659e6335219f5ad3f43ba20cf6fba70a31fa3dcf86ded915a41d1a8b99d87582
    6ab7b8f6d4896c092029bf3aded77428a22a56640215b550a6536e5eba9ce885
    5c7d826bbcded81d9ba83a5e4ade9e280374f95158ae382c3d0e57373a90dfe0
    c9f69c438a5fb13af3f7acbaa2c0970873aa69a0e6ae30f40e49cfe37d7c8fa6
    bb954ff3d642aad7a1b57f50e57ad89674d313c41ae594df1bc8bac1d4175c88
    118741672dd5b36b3e2856a91d02b0f4842bd21810887f7269e00bde1673d7ce
    c3525235eefa62e675bb6ec4ad035967acdf3be81ec1ccadbc9b8caebd49cc42
    5af43ae73c959ce8ed1c86284eddde1e85d9d32025f87f20c68afaf041f8ab2f
    7d8805bcd7d6f84dce2eac651fe3da6c1088f184421f417eaf764a62ec8b7e0f
    5640ffb330d5a3410f6a75e9285f76688c1558204cf6483a1456628de98669d6
    7f149eae88c52d87ff85e9b7abd1fba49aeb49e7a939d910b531c266dd9a6eff
    8fc31aa7dc298a140e46548ff6c209aebd0863b974f3d229068fbb8d6a677e69
    4ed0eb27f1aa1ba089448ae6432a571300377141a0171222a1d203c6c3d92134
    9a2ed6e0e0d50f5e128c00915b299686'
  ])
```

Figure 5: 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 the Bundeswehr Munich
85577 Neubiberg
Germany
Email: hannes.tschofenig@gmx.net