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

M. Prorock
mesur.io
O. Steele
Tradeverifyd
H. Tschofenig
UniBw M.
15 May 2026

SLH-DSA for JOSE and COSE
draft-ietf-cose-sphincs-plus-08

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

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

Table 2: COSE Algorithms for SLH-DSA

[FIPS-205] defines twelve parameter sets in total, across three NIST security categories (1, 3, 5), two hash function families (SHA2 and SHAKE), and two size/speed tradeoffs (small s and fast f). This document registers only the two NIST Category 1, "small" parameter sets - one for each hash function family. Limiting the initial registration to a small, symmetric set is intended to maximize interoperability among early implementations and to keep the JOSE and COSE registries focused.

Future documents may register additional SLH-DSA parameter sets — including higher security categories or the "fast" variants — as deployment experience identifies the need.

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, namely SLH-DSA-SHA2-128s and SLH-DSA-SHAKE-128s, 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. Signing and Verification

Signatures are produced and verified using the procedures defined in [FIPS-205]. The SLH-DSA signing function takes a context string ctx as input. For the algorithms registered in this document, the ctx parameter MUST be the empty string. Implementations that produce or accept a non-empty ctx value will not interoperate.

Signatures are encoded as the byte strings produced by the signature generation algorithms in [FIPS-205]. When producing JSON Web Signatures, the signature byte strings are base64url encoded. When producing COSE signatures, no encoding is needed; see Section 4 of [RFC9052] for more details on how COSE signatures are created.

6. 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.

6.1. Pre-Hash and Hashing Considerations

[FIPS-205] defines two variants of the signature scheme: SLH-DSA, which takes the message directly as input, and HashSLH-DSA, which applies an external pre-hash to the message before invocation. This document specifies only SLH-DSA for use with JOSE and COSE. HashSLH-DSA is out of scope.

A key identified by an SLH-DSA algorithm identifier defined in this document MUST NOT be used to generate or verify a HashSLH-DSA signature, and vice versa. The same constraint is described for X.509 deployments in [RFC9909].

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.

For many JOSE and 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 equivalent to HashSLH-DSA. HashSLH-DSA binds the identity of the pre-hash function into the signature through a domain separator inside the signing algorithm; Hash Envelope carries the digest and the digest algorithm at the COSE layer, outside the signature’s domain separator.

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.

6.2. 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.

6.3. 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

6.4. Deterministic and Randomized Signing

[FIPS-205] permits both deterministic and randomized (hedged) signing. The choice of mode is implementation-defined; signatures produced under either mode are verifiable with the same public key, and verifiers cannot and need not distinguish them.

Deterministic signing is simpler and removes a runtime dependency on a random number generator at signing time. Randomized signing offers improved resistance to fault and side-channel attacks that target the signing operation, at the cost of requiring a high-quality random source on every invocation.

Implementations that select randomized signing MUST source the per-signature randomness from a trusted and cryptographically secure source as described in Section 9.2 of [FIPS-205].

6.5. Randomness considerations

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

7. IANA Considerations

7.1. 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].

7.1.1. 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

7.1.2. 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

7.2. 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].

7.2.1. 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]

7.2.2. 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]

8. References

8.1. 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>.

8.2. 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>.

[RFC9909] Bashiri, K., Fluhrer, S., Gazdag, S., Van Geest, D., and S. Kousidis, "Internet X.509 Public Key Infrastructure -- Algorithm Identifiers for the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)", RFC 9909, DOI 10.17487/RFC9909, December 2025, <https://www.rfc-editor.org/rfc/rfc9909>.

Appendix A. Examples

These examples were generated using Cloudflare CIRCL and cross-validated against the Trail of Bits go-slh-dsa implementation. Source code is available in the examples/ directory.

A.1. JOSE

A.1.1. SLH-DSA-SHA2-128s


```
{
  "alg": "SLH-DSA-SHA2-128s",
  "kid": "slh-dsa-sha2-128s-kid",
  "kty": "AKP",
  "priv": "P1d2M4reQEEt09DkH_hmBUPH5mb12TZkfdp6rs2oXjmDHSYmLJWnKQZRp2I6JmQaXPjlAQXhaDt
lSspnzER1ag",
  "pub": "gx0mJiyVpykGUadiOiZkGlz45QEF4Wg7ZUrKZ8xEdWo"
}
```


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


```
{
  "alg": "SLH-DSA-SHA2-128s",
  "kid": "slh-dsa-sha2-128s-kid",
  "kty": "AKP",
  "pub": "gx0mJiyVpykGUadiOiZkGlz45QEF4Wg7ZUrKZ8xEdWo"
}
```


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

A.1.2. SLH-DSA-SHAKE-128s


```
{
  "alg": "SLH-DSA-SHAKE-128s",
  "kid": "slh-dsa-shake-128s-kid",
  "kty": "AKP",
  "priv": "Kz9ljgHX1ryVS2nE7Z_KtfIagmK5Oep1CrBYQcgK75DzFnbI9OqaLaMaevKzl1WJDr3mOmUB9fF
g94rq3Lckug",
  "pub": "8xZ2yPTqmi2jGnrys5dViQ695jplAfXxYPeK6ty3JLo"
}
```


Figure 3: Example SLH-DSA-SHAKE-128s Private JSON Web Key


```
{
  "alg": "SLH-DSA-SHAKE-128s",
  "kid": "slh-dsa-shake-128s-kid",
  "kty": "AKP",
  "pub": "8xZ2yPTqmi2jGnrys5dViQ695jplAfXxYPeK6ty3JLo"
}
```

Figure 4: Example SLH-DSA-SHAKE-128s Public JSON Web Key

A.2. COSE

A.2.1. SLH-DSA-SHA2-128s

```
{
  / kty AKP                / 1: 7,
  / alg SLH-DSA-SHA2-128s  / 3: -51,
  / kid                    / 2: h'736c682d6473612d736861322d313238732d6b6964',
  / public key             / -1:
h'831d26262c95a7290651a7623a26641a5cf8e50105e1683b654aca67cc44756a',
  / private key            / -2:
h'3f5776338ade40412dd3d0e41ff8660543c7e666f5d936647dda7aaecda85e39
  831d26262c95a7290651a7623a26641a5cf8e50105e1683b654aca67cc44756a',
}
```

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

```
18([
  <<{
    / alg SLH-DSA-SHA2-128s / 1: -51,
  }>>,
  / unprotected / {},
  / payload / h'66616b65',
  / signature /
h'88a36aae95778da5bce3a58808d3fe54b2be969d221d1dff264711598f4b5b32
  ee27ff1397233805989c5934e5766704a1129390ceb3d937be78463d39cf60e2
  4b3c74dadabc7f748da72343844c6a4efb5f829d4025e7be2be63afdeade06a6
  447f3eb884e8df9ca0a10625f7216b12eb75831259183d0fe9b9d6fda4754f6a
  4639646a7bb535338bcba2ffd57812398090f0b6ba9f59fc10478e67e4fcbe06
  5e04c6b371d8a1ef3a75d9871c004d8913929d91d53d6e22ee65401dafd057a1
  6c6adc1de25334940e40624d28bbadad502a531a039d108c195018759cfabdb4
  c97bfd6a40bd0902b3861689f79fed9d551330a76addef62077c2a5cbfc59db2
  d0bef40b313d131f475d6663ed8951483e63249e990ec4c15f99543aeb0af83d
  3491bb7f6c2eed57bedcd87f069303a6e18a188c37c8ca1b1292fb7a1e43479e
  9926457f8acd48818a2cac09dbd1b547467495374f82a5fd9be123f8b01489cd
  edc3b12757c5678944fcb3817c5c7ebe41a6834cec35723dd7d755d1bf127037
  23d5d97101e3d9571dee5f45f55771428058d7e9ba8d49d90e0707d8840d6bde
  94069bab7226ce6d3209e7a84bc61a85bc6236148d8421d7ace6fceab99e1ca4
  f0c8900b2db4a2fbad74e2dbb895d870a6d301e68cf9fb3e87d3afd06e8bade1
  535e41511e5bda2e2d1d1b2167f90b6d64a0961b23e65c90323419708261dc3f
  5d85b847f8fcd080e6fbf0a3ef1faa496cd704399f8cdd14f9c8c9b2e39dbb84
  3d6a21fdfef3c2f6ff955da15a1b4d8d8b317caa957965865b6ca64cb9055fce
  9541796fb02f9c31680e230dc5b2497a595b91e9721c26f4427495a162bcb4b3
  18a55303a05a7089a72debb5b034a67d5338e80ae4b4d903b26c98f906e9611c
  6e87e666a15854d1248f2ccc6a736c42c3f9212f300b587da1f8563938838b5f
  63d00c19d89e951fe7c10647e652dc9e91408f66e03bdf087c893494085c7dd9
```

```
f63cefdb4b69ca99bdf1a647dff354e0e0fb96eaa38922e6fe1001a9a3be2513
90f2506de734a84ccc3e74fd9fe2c9de72ab01462112a390607662c158022642
76b1140473cb3766e36d86568e2a15cd0977d7df2711eee96bdb32e4fe66d9a7
7ccc21ddd36c4a5b4b436b77ea783ca982a17b03b9d55e144e699d83b7f9218e
68d609a93fbec8695770d1ec27dbaa6e162d635c419ff0fd310f46b8c8a1bba2
4dcf10e23aee5519a40f123d19f42807fdf97a7084c7b7da84882c267da1a1de
c28e3a3b7c0f41f1da95f21551acdf55b72511d7ed2e7de7d13a2382b23feb96
cc2d0dd4bbabef64cd59e67145a94dd02934d75d263bd5a58c7342e9f5815b53
7ccc7f11545c182d665c7feb87370132a290cfabb26ea73d98e2b51c607a5824
1e88a324bc4cb099017700846e9884b993d319fa3298e306a484dcb72bf6261d
b40cfa52050c2133fa5fc0eaa3f84004a85a718a86aa6c70f7b4065ac43ae5b9
7fd294870ad08b6d06b60705c6486b9c447e3510c2a17d9b8640dfce6b190bd1
83fc46da15c79bc4dc91e0c93d31ead9e4316342273c65548ecb5e623212f021
ed460e3f590e84ea8c3040010fabe9b9b86eb1100f8b683d654b4b73c524ed24
219a1af97a48881d7c6db5fbd8927b6199229afc0613eac26008bca53c592876
01acdd0ba01aee865068670354d91e58447b36cb55b3c5855d21798991223874
1e39ee0f6ad64d3f06d4a4c2ef833ede9cb1e5aefe722e92ab86b0a455d3e49f
042d0320b0e27dd1671e7973c113913e598147e0c440a4670616c9c5c7d98d2e
8c9e3f1bf7994b1d9fc0fc347961e815917a6e5dd61ebe959fcb848b012dae9a
93378eae530522c52e356bb75ff6e35d1cda32dfaac9e413ef35152af038cb2b
84ed949d34e8352d263f4577dfed00190d6ecc8e8ab4a62d952723c1f86891d3
e16ee0af156496446158a97f77868655f8d0d7cf6c1c140bbd94ba1b847cf1f0
96d09351737f4b01f2579e9a999cbf913d91062ca1094e32be3d6aa029cdf5bf
7d466d78fc1b12e053b749f5f29fd9edde181cbac566998ac82a1b72aa348d2b
4aaa0376e2fd6f9331d93014d22b26d72ae3dbdde8987df5f4d7e50e8cb00bd5
18c50a8f8dfa517131aace8817f3dab5918d45a531d59050b2394115c022653f
abf38d5212415ebc30605f0b65dc5159d1f9676382122f5f5d7f7a920fb7031a
36b594416367de00cbdcbe33482d8850494d32ea3a2f564e773e2df7cb4baf7c
1b809a059f43e83bce8dae0180f295153b524bbfbfb20ab9ff263fad2b90c283
a654fd6d6b04e2bfd08a3c7ee5688017eb122a75146a82d201e92578959cdd39
582044e341261f71cf6a04c3f29e1cb2acb317ecaa440b5b7bb75e3d500d2a01
442b1a7c73a863d8b57697c86345b726d14e20826ebf1856890e986c3a3f5d39
6e6b6280768a35c686606e5b7037dc7292baf68f21f2c7c511244ff186161852
0e6dd748effe679fcb404e3a156ce87e87df5971eb45cfda5ac6f18656b60840
40073137f0964d8a26cdc676be89433c3adf5b32dda284e1e0bcece0844a734f
e41afd378e28082d9f4d1df3a02d19bff6bee8e5a70a4e53b70378e924afc839
53c44d1a7293fda343ee35b9eb657e209dcd03a66ca86d81dafe091e2f1d287f
cff194cb6651f069dd94623fc1ab2b4a8fd74758c6f6397faed6f36d8f21a18a
b047c38fcc002ff2b1d48ba424b822954bdc3caf6a6b1ac41465e679197acdb8
0abf5c15c7bcacd03c0ac52db7b07e07d1c4ebf1c5bcd12bf56e3c66b1d4d21f
c6b7aa5bca1a9c1532e9c36a93e8df89324bf8bd19fe6a1cb195a3e78876bb32
d0f876f4d93d3dda9c7bd3641c6ddccb901b325c47aa8ca6c6507dad01ca156f
6a9bed201e64441a0fa95067e8b3c114ae523b28dde4ea3f0acd00ae4d2c359e
3fac565f795a5602f11b2fcaa0c1b025b17142eb8b00b71fe784ba5c53e142b0
e79f4a72accdb6efc05866da04d70c44085dd3996b17527d1e8be143d0e7f1dc
c5653b9595b13397b462d0c6706c557db2bbdc360557357ce87a67b61be72ef1
3a865ec316d5a0f39fa66d49bf67a8b560b6d93f2c941b08c883c0610b44d073
9c297ef0308d12725310b4958cca48b18336060c3bc496322aaac08ef58a6deb
```

```
0c46e0f7001dd9d1824ea9b948abaa88baad908af4d57b2ff6c200ee41ab3d0a
ca362491ffa9334023a841c6581e2cdd1e94e03659a6564985dcfdb9369333d0
82c53a95003dc108e5c6e11cf46b49aa42125f35e3e99b2c05f6b5c083678c2d
1a5830924c3e64ff0e43722ec8882a25018b1da760460e53c15034f981979095
308775f181cc4a72835155e6cecd8810d813834bc12c652f10f739fccdbcf2ea
f30a840530495cc85d2e9a7334f491757d321313526ec32f247c49a554d064b9
802eb70af34756198203ae49d4a25cd72fdb638943268f25f91596005f9c35d4
ed1990d813e918558075fb7f19c37c578c2eced5321709e790f7f7244cf95892
234f1ae5ee5703c5302080d29b9fe04edd9f7f94fc97aa8830c052dff84f1386
42ffe274c09e2a51d5ae740f9d8d1bb7a990b9107bae7b44bf8737bff65172d8
becbbca74dc521b78076fb2ccb478117dff8854a1d9319a0832bc1ffbe25ae05
1f43c8c7552a777ebac6b32baf6496e4badf3106fc5a59e41905b7a33ccd9d52
cc19133e10952a95f46ebff8ad1eb9e5fc48037a5e1909a2919ffb45d0d96ac2
66bd6e3b6cd6d71159f6a9f8db0244729212c7c63f82c12dba57cb7829dc8469
cf538ac133972fb343d4a3edcb0dc9fafe07f759288fd584fa7065e4c49e305a
c51cbd833eac90610c4af3e3d5f718438e9c3b372a9173ff8258eda02e6411ac
e862eb0d136f2e4519264e175c2d1ad26452c832b57a0fec88f774ba4e85e901
0fc02bf901d1613f91ed997708889beefe3be5e5b29eaf89f13e3287d32c8801
73f5a531b11cfb4cd66d617ccea69dd0ae35ffd7ae94cc612ad01be0d7d16099
35a0b621bccb5a88081bdccbf41d555ed1d1349b556986e4e9944fd933498f9f
8472a373dd77c6ef05b3f6e7285c4c0e8c936a536d1683ba00f07028b57e0d29
ed9e6f37542c7e937a345481f9088e93c410068d07f6a0735d2981f7f053f5e5
ab9b3e1ec549a3f1ef65ca586d303960f9921d4bfab4314e806580d010a630fa
aa000db19b1575ae854a38c28d8e80c339571395e672e0d1f9800caaf472e234
d80080015b9fd5e47094297d8e529748bbdbaf506f2ae2b1e7faa4e155a714de
081c40e1d0bb3f5e1f9874a243cc2e060fd6ce2e60c1573f163929a3a017ed0c
fcf5869ff92a03376a761458480843bec8536844383c32055ffb863b744be2d
da228fdbf4b3d0f6133e07d9bafe1dd16ee8b4a0c71d74e3bf7d8d28fd6ea476
6e1ddb894e8bb213526d411e02d17741a064153d2a9fa9b09d442f1118ffe7d3
a376a07e7b184f61145cd007f92550e4641a9626c676ab58f3b23d791fb2ee8f
bf70e080c0f1aaa70657c89ce192121ecc15568d59d16f67f10a31f2e5dc12ac
037437b9735e56bb4b05752b31c5f91d25af9ab4f476ca08f8afa92022224ba8
f2a645974999453e297b267addecd55207f403c310628dcbdc7f20f982fdae5e
750b97a70bb296fbc846a58f460c32d3a39e249f1e2cd776eb556a5a8b5aa49b
42074a36972da7dbf4cfd1349fbf3f62e5dddd8f1397a58d87d5b78b99b6cf32
9d5dca35d17d4f2d51ba49bda6c15a0642be3030186b992a6776ae26f08d80fd
f7528581acdbc186c416ac5cea97cee6f5242ba7f45a6339bfd1c57c4f1c23b2
fc1da8853ada7e2cbf1a9c328a8899d22b043daf00ebb14199e2606bda2d9889
b4ba27c643817acbe2f4ae85a728a89d111e84b9b1a858e1983194e060ac3218
d2583896f5672e1f0c736bd54edf70ebb5208de7e16cef9c5f0f8e11069997da
5cdcfceed7afabdf27659c1af411d259735c54c35cea1d263674c0381c0de957
fc307033c7e853c8cd68f55fb02ad978f027297aca6694d894cf54c28d7e6d68
2f7ac64e144514a4d9350aa8bc07bea3d933796cde3f75e2595e961963c1cccc
13aa6292262d74ec9cdd8bbcd3e49b07cb5808344e60eae6edb0b86f5644338d
a33cdb9f9b8b976b3721ee6e29d940c908f43250bd93ef737983eca5f5324e07
1f1dd8efa65aa8933c85fb847aaf195b893c6d04c4046230f2f152d238c0fa72
d60f7340393c8393e091edc46b8622dd55b336b0ae695009d5abfec5ca9fd697
70132f4f7bf3eb14983aa382f65c1944d3c07bbf0cb41712275aebfa5d210de9
```

```
dd2b13bd4273ccb24e74a08bc62ac24dd614a70413a30e5ed73230171b2c3e4a
5bddbb1202bbc88e045f987f3ec15da7e06fbb76d16bf9f521d77ff108480399
57a3ef9bf8741fe23f2f723cb97bb2a4941f471d9769260790b446ff46e831fd
345a54809f86680af504f5fbb08e3257d1ef277ed44f7bc2a31d5222bf0579c6
b4b416732e0bb8682113581b6f5c68a9eb08b355a8185e110983ea39974f6464
cbb6c60a6690b64fade97f223c8c498d727ad312459f3bf115b26afe5f3aa523
84d60bc5d1b27ebb2feae90fff01cc046eb81d6e9fc4e5860263e0624a8d64ef
9ecac0ad97ff6610eeeceb082df97f59b15c94dbcd31e9d2fdfa5efc23fd895b
342d48e889082411991a7f99d183ea6abe7ca4ddd03ccd496ba7421d54e157b8
246111fea7ec52e74a3e37248ecd9e17a02b950a61ab5a98bc078d269f03f0dc
f911702341e2aceb5a4717d66accedfad2124b4a37f764a9221b3dc0e7fe0eda
cb3ba335d23778ebfc86d6c74f786411c94c6c3e0e63b7393888ae372d3922ba
61ac39ae2ba3723ba5da1bfdeaf6780c38c1c228f1f464dcd87545b58b318b6e
a86cc7d6962d4d7c4977cf372a3a9cf2c1c5c96cac835427115ba6ca97e45a60
93e4b1d80fe3aeda0e7d392906804dcefd19689b68ff99d8fb2673a4046fbe5a
74072be0d1723fb4c7ea9ac96319ae45c8225879bda5093b642be35001cadcbf
ac5f71001325319bc10326b6a7b2d30ec6b81f10bb9fe3c8746b627cdcba6631
5ce235ea3c06e2014de6d1b5154e49374791bfa12846063bbddfbf3e7d5f78d3
be1b05da68a594ff12364597964a2ef5390da36d0da26672a5e5b54e1f20c103
c8cb5e4def9bcb3ac41decc626d714e95ec22af39fb5876f42c57ee0cbd73590
1857d76c2a12b1efc7332e2b044088018695dc37cc4ac31f1054390adfcb084f
6ff3940ec2ce224252bf8973e74be3845b5fe01b06805729818dacc6e5a7a3b0
167e6b8649f813e7637d89e374b5c63ec0ba97c744c2994ea00d6d4c8f4e3b3a
811dd4cfb66944b208f0346ddd5c6a74a70dd4fffeb9ca9eaea4fc83aafae600
f434c1672f59143e4e8ca1c823ccf23817561d1fb5c1c9f1a484fecf83297064
52d8a0c9e4c2bb4967a69ea8ae9e51227a42924d692b6604ce2d79a505ec5f60
4bc3ae5149f2860197be65b202be1b2d2c1f84377e26a900ff03c4994bdee164
cfcb062b0c34868ce588e83c3b962ec555665ab347d28f4f9db91ce1725d30bc
c1f7abfdd1908d1745dc248b3cacc466444b0d53a3bbf8403af3487ebcc29b0e
e3a0c75cdb38472cfd34e674f46f5a38dd6d41b6bf2ceb9ed7298802789932e1
ac2360aff9f8a0a2fb4e61bbf0b7bab52b6a71460f08749f71c6a08a961fcb65
46edc227ab181a746ce9ff89c3a2761cf66696fc999ca9663284add7bc4d0a04
e91e03e504b46d236013b1cc54b46a97f3424161efb8236f66c79ccc6370b2d5
b1e925bc63d94e4873606c76edeebef01e2123c5973e06fb6330bb13633c7e70
23896f1b75d042b657bfb41afe9d75d7b418f5ce10f5eaddfe1b129ada7efc01
7783214d20d556cd73da01fde08a3bdb472be4e91f55012ac3802eefabc4a74a
4875b9a8e6d30174238802e14e99e107fca36db4aa713a4d434c340289b8c281
f1b7b54443a03808ef1947352a1c85ca339f31f11d7beb3c13c63bdd6219c085
bb0aff791bb78fd9f86a7dd65b92604bedfd2f510c66e46f40f67fb1a99d5330
db5d946ca093ca2d1a724f90991675aed3fdfd9137aa39dcd96279b5b91439bd
9f2f7bdd501775fba3ec867d66b304fda05b891035ea4fd26da33de4b4aa6382
2c6fd34444e1a4a81c484ec461c519995e65cf945e214f43cf57396323d48281
379fd26744c4888de2b3c342c592835c69024744f3e534fbcce7f93fe28bd0a7
6d1772fc71cc3c5015b462ab1195e6c375a4e4f51ca13b7bd99f3222b38d298c
304bfa1bce76bb29044ade25188fb6921758baa60c29b02773acfa5f9ba5e09d
1bc926c2e4aa6198b1d75837fde1b6e773041059f899f3184a8870064f5256d1
e026a665772172e99e25f531508615e16d033558125c706bb5f423a218b6be10
763f72ae74a12ae19c9a308d3e8f0ec858bbd20ba3f53b4646bad46010334acc
```

```
63cdec304a497d4ca472238ccc083bbff82b693cfab2bed3c4e93e213f9f4e4c
24e730589522ad8af95b9f10a62ce39a19e9d7e10d3a81edfb71f70d1d630999
e7e5adbd1b6f51c62bb00fac1c1bce855884c606718e40f3136944d129cb1b8d
a52e3ed5a0c9092db940fed799f46c4ea8fae0776f7463d07724a27b67e9b20d
3eb67aa7b2c2640073fe8783893c4ac3618087eb80035969c5b590a901efb32a
dc2582f2f1a4ccfe0aac6071f620f625083d1aedf7c23c311d500c2f31f775ae
870974792f32a3c035a86fff4126f5937f4042583a07fcc5b4a2f8251cce74ed
548ac4509635188f7d1cedc652727f4dda9cd0076b2121e722a4c0be400972ea
d0114690b5d3c2bb3321435115a1120bbdfc9405980aafd83f33aca276269d79
78322761d51658e15fda3c6214400bd3fca1d6ccc81e5d4c0e7cf5922856ee91
93fefc8298b355e90642a730ced43c04abc8c86ca14dc62d84afdf144ce092e7
900721f1b59604671a03548b2a1c0fac79adb7b9977f0eccb1948368f8ff3414
173cbf3f6d49d3de44042a698f36a6764f1f5ae7b400e5fce9c914f80009ffa3
f4d72e5b3ef00ab450bad3f3e92c430022bc6b3fd3e04d628feb71cf2a1fd5bd
ce840409d50d87a0019f57a19f238b685e2c51faad078f4be4b7bedd9e1fc7d6
d200f3cd09edce7194a140136de7b959371f2741bf628226b45059ae4db30489
8593b0bd52f32d9b045eee89db5009f8526d3f39b87ed803c1de89041bcf4960
960f40f674b2fe7db448ac8e18690ad6a53d3f90e8229c4fb23f682a570b53f3
4e180e5cc7ead81c960ce69324e2af46d17872fbadd4d9a7a1fbb739ab6e0f30
3eaabc0d97a17375998b0fbac9a1ad3a3925997f7202ef35ec9a9df1d137734b
e71e4ebe170f4f02073c65613c6327e297d5a9025dfdd369afda594936e0162e
97f7941d3a2ffbeaa6a3ec3829e7077959a0754cfc23affbb9425981e3902579
c47a54c90ccfd3ca2b0965a4941404fb8f75dcd920a3f95661957004031c55ca
2dd709b8d682daa9f42bfd890a375fc70fcb530571fd00e00f30051d70c9e0d5
30576e2bb778e3e2e7d6b9101220d9f690dee7c09158dbc2b69ae86b30e15819
5c5254b705e102f3035a10afafe8b159daac7ab94eadb90f360fa99b8a589550
8ab9efa5427a8208ad3178245e6f0c7e75e5b8093b1112e6114b39d2d10325c2
6bf27ca1aef655b46ab59cb7ebbac259b702664d4a0929b85145e0d0ad5ceb86
360ca8492b6e2f3149fd31ac24c75d6f830537ab42959b7b1b2d0d2ee7a1457a
78c56d41714d642987ae1e174ec97593979693acb3b900eef2b37bfb8efc5974
76a820eb1d650dc686fec4edbbe505f48d41a64ffe0a3f83091210b452d75493
c1876e1d665160d64413f741cff8e548dd7bfab849d8d0a2f1ffecba25a05d68
e75be097ae1fb3d689816a730a35d1808f2f09cb662a88a3ec4af012e914fc60
8a0cda6f4d72c0ff1ae61e7a8a3a0d27e9e301ac34dd9cee238e1a97674ff7a0
b75ff92671ecff772d3b94236839e07604ceb2d10bfba2ce48760295045e2340
0cc82c760ea2b794f49cc89f26b04c96f9c4b2fcffbab3c059269a1e2f921768
90137f060ef579d4bedc20a4990dddac08bedbd542d75e6ced0b2f4aae62eb44
4070c10ec802dd2a96bcd7084b04a2c38099de296587644edad962a2c5797b1d
244e7a68c5451db429457ddbf1c09fe5dd01f69a22b345c4e85746fdb1ec211f
5c09721c7f7dfbedb11fff7ebc5c3757e61d045e1412d66fc9a26ce64ace27ea
dc45d0e300274f4b439d59de7a84c38dc39f31ec28429fd6c5900a0001e84b7e
d492261264bde0dacaaf4a0074e76533dcbf90d1d58b34e930f71d4bfbbcac12
74ed581ab9ef0a63a3c5b34e260fe7b6decc6a232c42214ceeb91c0008cb8c40
f2ea1e4ddc1774168ef969a94b3fed54117df1a1f4bfd7675163db7632cae4ee
fdfe9d373bd4d92689ef3d7efd9f053f9fc58c5789881aa8c47bc9247f013938
8e3e954d1796f15e8d10ec64cf8681198d80b49c553902ab963ed6a316c6f996
cebad946aa2bf817c9c80c5f1d212a7b9fb81565a94c2d1df58b0b9a566dfa85
ca1808f9354df13eb37addc9eff672c5f654468fdcc2a326a6eb340fe0c05e94
```

```
    ac55dfb51b327725bddb686941f478aee909d0f0a3390832a94eea30d9b3d592
    54f2f2e8416fa3870acf69de5dc0973d2f64a35e4c39bc66c903ab0ea7b7d6a4
    2e7c763996076afe95d8f6510114008a2916ca73a27946c7abc3e8580371237b
    a338116459d0d4c87dfa88d429606145bb1533a62fa5b99d638595892da6ab1f
    ee27650319895c5305f7c35798b917fd5a893c4e82086a86d54c462b34266887
    e5d88a942b53eba36970eff96cfa994cc4400fbd9ef5430a3634fdf3d66273b9
    b0e79241a56e1f1262b45a8e1c1a7d76309ce7c3f24567787e8e2afa5183e5e9
    fe35098037d202bce71f157503821824fdaceebc6505dc67aa34df18cab427b1
    d2b2b280bfdc4ff41c1b409a3d1dfbf5cb2aba11ab0517c0cc38d81ad5c9f14f
    5b7913a0d68e340da007d7d266791547ec65875e8796bdf77dd2c7d7b3ff61a3
    70ded262934f3c099f0755f026ef544bc03c6f65c6770dc0291427cef9b3aca9
    d3976a27c6cc333d3a7af98a461ad7103eba972cc815269fcddfb55c201654f5
    d911e288a7e70f08e45831590d5020978637691630397c0ff900c9a2bc5af210
    a88017970677bba746258e518f4b07045e3f7ef45fa6e8d795ac6a554f4b13c9
    49e9e68b6d7ac8d89104cddf41e09e85150bf491a9028a57b557d7abd75d8f18
    34c04b160660a3ba7853c48d143a88db060b819ee916fa04405e89d70a4757fd
    9db44e44cf9ec4677b3082d8c078b00af0f758b499e5f30671693ac3694ed073
    84bed05acfa72e4582792523f02b0328798396d6cc6261f1af3842a864b4de03
    1a1ba8e34fb39501b98ef1a93bc83812a1dd5537ae0daca82641333e8858edc7
    d2f512b346485bf453d7b06740e60dc714e550824fb48a639688bddc8cec3413
    ff51d930d597593eee077aa5944c57e29c4462436391e27931224534c8d0f9fc
    140a49fe8f8287ada058c25e90f22f6c56566d2885a7cb4865f5fe278bb6ac5c
    7956f6f52b0d3162ba7252165a03b3e4be7411261da512b8f7e8d62854cccbc7
    825575deda52fbc1e7df55c32e1e0a83b8c283c146cd39352af17290b92e8ae3
    64290c19a6a02e0c79f09fe8b1e641aca0efa62cf843e1c8522b0e6451b9a4cf
    c45be3e6138d00ebab66f3ff8a822a633ee2b6dfcc9452fc240e17fbe0fe7855
    156df3501068032b59326203e94cabeb754fce6b9248c809755853b9831381b7
    25d5ec76da35bec90b884297a4c7b11e237b333d075b821b64e837f31e522851
    2ae5d22eded5a3ee4b6ae1d1753e78cf89dc9640880dd3f7f08d75be2a3705eb
    118ae36d099639ce456508adad6c5bc7b725f9a7e651e3a5e7ada03731e38b5c
    fc3d16d7f0c10f5ee6ff130ef2afabb3da3317d10ebe8d7c0d9cfe1928f865c3
    7883a014f086d574cfc160b8c8067244',
  ])
```

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

A.2.2. SLH-DSA-SHAKE-128s

```
  {
    / kty AKP                / 1: 7,
    / alg SLH-DSA-SHAKE-128s / 3: -52,
    / kid                    / 2: h'736c682d6473612d7368616b652d313238732d6b6964',
    / public key             / -1:
  h'f31676c8f4ea9a2da31a7af2b39755890ebde63a6501f5f160f78aeadcb724ba',
    / private key            / -2:
  h'2b3f658e01d7d6bc954b69c4ed9fcab5f21a8262b939ea750ab05841c80aef90
    f31676c8f4ea9a2da31a7af2b39755890ebde63a6501f5f160f78aeadcb724ba',
  }
```

Figure 7: Example SLH-DSA-SHAKE-128s COSE Key

```
18([
  <<{
    / alg SLH-DSA-SHAKE-128s / 1: -52,
  }>>,
  / unprotected / {},
  / payload / h'66616b65',
  / signature /
h'739b331fcf62683408d06d279d0726b9cd7ecb471768954695b5ec90d16888f9
  f49aeb20cf27c4c3af7e18307af67904043a786b17511aa9fe1b88edf45e1e6f
  1d3985c2812a27f3a27047af1237bbd084c47740d7961cc3d7cb8c62402e5b70
  c22ee5bdaeabe25e100d8819dce0b84ccf20c97fdeb81c5d0feeaedb5b5cac4e
  a5aa10f06707b524f4abd3c137f1aa136d80e30e53b8c92c1c1c32b76042e1df
  eb163f3fdb9b0e19fa867793e1c2c09f41084015e2a269a63e649c8e3fae30a8
  3352215d517421d25d8604841ed130055f7c931c375bad32c01e40ad980dfbf0
  1cf99fde19ba3b155266ae33bafcc4e5d33a7d2ff585fd016d5c0e610e77e940
  97adb10e897d6257faca3e72e329fa73a93627b8f118926a502b4628879732b5
  195880ee2b9dfb6ac2fc724238fa108a871c6a02ac18b2d976ee621c3b38ce82
  46c9826e596c5e14d2f716721aec7648ccb0953699b77baafbaee343ddd06471
  aa28d6f48c7c5f0b772877c832cab4f970e1ea832aa449db07a63d065867c02c
  3f9783e96732337f9d93fcff16202cbdd41a326aa65fec2e9ea239b276ffe08f
  49f828b190945ae577ff71dbb46384e1f56bd9e44dda52e9df5b9f236b42cf17
  96543639b6795588c19097d211582020fecb1e50cb22190911378a15d0784418
  4ad3ba1c02011202c636d1e4d7062f854c6003e1aebe79571615e95c50dd49ca
  b1eac35884272244d463c7d0a2c97f2c611ed14525a09cd10a3fe1338ec207b1
  355776b655b68e474a70d8453b73410c6a296305093ab476f59c7258763f8f1d
  6c8dab1eeb56910398535e97a4ab34d8002337abb967454b52320eca2c7478fc
  0a962a09c1531f26055da531a1c81283d6788f9f4095ad372c94d5c21b2753b9
  9d57baac19b9be3ea0c2eb53076386d9b52af8fde83edeaa3b61d832edafccf8
  c94d36f756f358ae5e1afdb548c27f479a399b23d3796c76a3298abd98894675
  6ed0663e18d693bd5876294b5ba41d6425cf1589306cc9c4d8d0807701911cdf
  0ccb1294477856e9e0d53ca486ef6df198c6a544011f819253a822bf8ca4ed38
  812135dedfabe9ee6aec72bd3db015b6448e719c69d8491a63e85f3a925c7c2a
  b0e53cf90d6d60bbf8d3e1d881024f9b53a2de46fefd8efad201b437b07176a5
  dff36af82b928ced03932a74cda4d166f63a9182de858cd5a399711947de2990
  2fde843b0e5624980be500dfb2fcf1ea4c56550ce4e53d1aef035f18e2e2f3af
  1e9311baac001d66314abbf0ff9761a56f6eecd1c6153986119854143205 6f47
  5a8bc52c1ebf04fda92365f6d1c0449d28491fc397d4bc64dc3093280ea51844
  9657ea82d472a220589d11ef12733720bd18245bc92c8e5e0cb23d4c5cbcbfd3
  cc469962094ecfcacf818b3df113ff6b039b5b260e354f729902700b9fde4da3
  cdc47e5f8dae03c5ded6774b818075a4b407ebd02195088fc34f486346bfc163
  b2fc0aa7ebce86ce9c8fcd1bbdbe3bba26557632627701c9946f1278a7834a86
  325dbec8e67cd09aefecd487b2abf12b51bfcbf6dc93a9efe120fe985039ec6d
  f17c8bf6fc491116c2ba10d1e2d6d43394ad521e174319cf3612c6238ec51d97
  439cd929a9e62da1a04e092cc7072aae9f357cea46d2907e4ce1aff9ce290f29
  7984ac331309fb648b699bb684af83ad6848ee9345399c12bac2900660b56da7
  7ec58ee4078762c04de1df9a32652ec2918933f3e749762221f5181b7f986154
```

```
7177d0466fb6465a3c2b3b3f915d1525383ced45ecf656f1ae4e1618bb43b6f8
cd194eec2fb835bb1db426cb358d1eb566abe87eaec12e1c51b2c6a5f782da63
bae4ab2dfa33e2d6e9607cc46e07ad7f1914cff4cf8bbf9e4b53a53c333b461d
fb83732af3bc7dfcf8acdbcaf0ed65cfddbad730f0a99e989041ca4a46791c74
0f7a129f24a085300a36162c716bf2bbe43f072e9813dc09c1d31006e5994da1
ca96fc8ed90eeaebdb41257625faac41aeb1ab8e9ceb0404c88df5ecdd9d7dac
686b2240e34c97461e0f1b6b7e98cee022279ee038958bf261ff5ea86ce091e1
966c8a877aadda02e47083593c95f0533e157c558725aa6830094fbcb68e0073
39bd144e271553eeb4d456f9d7b0c301a1d5f8fed8b0bd4b8212a4aa11c4e2cf
57ea7cbd5cd367398077ec46c2d900a37124584ff248a27695d236638e007965
b87d94150c078f168badc990ecfae215556677dfdbbc8b6e6407e82580e98ae6
3ba797f176495b45c41d13148ccf9db003809b193129ca356fc7abdfb1ac9bfe
686938cf46e20331bbae0490b48546b2e7dc7e4c618f333581f6688ec53927de
63fb84d01c3cfbc06e599a67e1501b11a4109668edd28479a02b27d4d77b6d4b
b35c902c7beb67d69bdf7c06fb8a51c6f63f719b837067d61961d2ab32347c8f
97dc469d89cf5e16f63c12dbeb86e573e922e6a3be40ecf292019df2b8d1de6e
593533e86b60ee746dfe23090f4daf4bd63d3d0553f07c537b36b1912bd43131
38ef1d027cf51785b910cc56d86e76791a710e07d0c1ff771b1af007eb24c0fd
bf28137f398cefe2c457844d3d607718324f964593b172978d17b4cf2a544b47
1fcfa085f48d18e5a3aba0eb7b9e2e1a0364875e768a580ec421950c8129642d
9676c661e4b28cd52272dafd125c259bc8ce26492094878f63239d2a01202c45
bb1f63e00e9b10509009b662ab434f7de3a567e760b9d83b4ff9091d00f1290b
47c7a4802971e6af37d1e0fe39bcbfa8f0285633c134a1242ff2d984fcfe37e0
29c8c3c6458fa2cabd9aa15df5d9fa6e9ca63678918ed96268236f8c3dbe3f58
13978a478ed5ac3a7b3ce0bb5a726cd478ba040f42542903c0e149166e5c747e
9959107f0615528345aa07f1afc186bd9d1f3ef2ef2f322936501ef8064da68a
b0fc13c72b2a110830db0e5257bb5cdff0706e8e80f1cd9d1438f4662149387f
c6430bdefa01e4dcc0730471ca6391d5300fc1a141492456bdd790c3a7eba19b
06a0fa937daf76ae7f2e8db7e82c82f891d549e62222d4adcef5428fa488e52a
3be7b8776e6706caf07e859fcec933fac12648cc63f7c0e47d971f09ada10004
0a4599f05b4afe609868113805fb30007273fc3649a737846f357d77e22c2f2d
9d9a66426d23933e28bb707b74233a35abb6fb82484b629d1280afce8a674b9f
96c5f186c9c63c95d0b53398e4ebd974cc18bb36b46ccc8098ab7e2979d9f7bf
3eb44416bec84b9f53a91f349562bcdbf01a3a65063f199066c509d013ecd2db
aba623c2791932954d9ec2ea2a1cef7ec17a5e4e354e77ba9b6ed6bb10346cb6
136c367fd8f6628b27854f736ab1001b27a3cf5f90d7fb8d8e52fe23481fe3be
c7ab75a1a3db4848e0f5b75cc1cd98815fabfa153ec042d1f421a71886ec6f62
c327ada1a525e487594f09d26fcb0f9348f3785ea0931e3e85efd884cafd4e72
cb1393630e81dcfb9c85adbc3193969b7be3839671dce37e3dd3b62c32f2be70
6b41ecf18508eaec6b9bb984a201446fb8e6e915c435d4c3297dec273f0782ac
8daff6978fb3119f8ef59a83b118fd918829e7e848af5a80f6a7ad20b7c7eedc
a1d2858026faccefe7038eb091ecd6b103f37b7c4d3074a7e2f0a635eccd2499
5fdab45d7104ab459191051e114501ddde2b2b3e3b7aaf803817a1a25dbf4bd9
cba34e6580a322b6d6c53487895e8fef084d7cb1cfedf2192116110352d81bd3
babe2bc2083c5ef0d6da10ff5e5b64fd3f5373489ec3844177e99265132fcc69
1cff9f71d58060c5746dc80c29901beaeaff1abff6c97df94d12c08951d201cc
32c8b13a3e7d976b9cdda5c44542713abbc1e4e10b4f477c617d44ad411bfc22
c7a5c0839d6dda428251943c812e8e46378c1a4fd705b7d089cccfe0307f5e15
```

```
65148be40535fc59d7e8685ef74db127c047d46be7e6450bc31810b74cf98782
f4e577f1f8c8cef1825261bff85837f2ead668313d92c90f7ef2fbe2fe334600
2938ead3692c8b017534139fe5d13d296bc9ef00c13321d7ec8f447b9099e78c
34e0ae8d6c0cff45657ad30e1f188084f60eac2f630fa468d4c9a7ca10502220
0e3e4062bda0389d0f046c47a20b05863a6da524dcc3cd6c6e2d0d4222256a9d
175d5cb252d978350138312a581d0ab2e9bb2b3d0318561c7cfcfe0633b90f1f
f59414f278b431a8e81831a0ccd49af613d62c85d8136af90552bb49786efe49
6cc04b2261e43057b1aca4f7e23e1a7f03304b956e59fdb2b88cfe2d91f35daf
5b9695d1f64c9ed51f0fc6a72c7c14383682b62709805afbe9a9bdf441bd851d
23f9284e392d5e115f48367f422bf0856a2f8c7a0c24aa82064e178331b9a987
ecaf07c40a0723608ceda6636e7d6b0bab16272f0331bd7a6916f7826df9bcb3
65a2ef60149790255283d6993ffce3478e26c7f69633a226bdac01066cf2b09a
db696d049e410902a2679a436a4832a126205a88a8dff9ad77f501ed8af7b54a
e73de901a2f9fa401aa41c57c499b3d1ecf849e0f6e523d47cc3482b3b34d46f
b100fb8987953d063c86dc952db736c6ad25d1c0cd8b6b10a91571d2fed91a25
400e4a6df18f85d48c539947a392eee9ef9db930464f239686a59e22ae2f1c17
108ce40381412bebb0fc21b9f5531ae5ae148df1439f7a70aabfbcf83795ed60
5ec1777e15575b772443f925d25bf35946368b0e0133b4e79223ab4eac8deacc
92eca85db24f9bee9abfdc16803709eede8909b024c6cba02b56b34f0d1ba19e
6ca7cd73dede662a4cde902d36c68ac0bb5069b0a8319f64de92e016b8e4fca7
a19fde3fcda60aa0225b3baec1017ec83315d48aa175947d4b02e9cc073547b0
dfd1a69142d590e63c237d4cfaaac18834d31008d7e516275e140c76c9df3e44
7aa3496ec633b6d72a06c7b0c6b6456fdbd56dc1152e6b7667384b3eb3c63b86
2e4f14261cf9861531b7631032fa2eee97f941feed85f042288564d2fa36fb42
c944b337844a1466170f13d8b58d5ef03f1e86da76863f3e813bfedd9283619e
263ab99d0549e5852700b87fb17ff70d8322323c13770c7489fdf5ff643a8d79
de62872d42dc2a8fd39c74fe98e98261345fb5b31486350c5a96e24f95e079e6
327857c99d502ab326c74f067521053e301754ef237084aa1ddb37d9faed3943
491cf21ecf1936c08a5150c1a9b405349e5bff757719b7651f38866ca40cf309
ec1364db6fac8984b2c6fbe97eac49599b22057babe5690950017f722e19e00b
33dace55cc537de9ffe935b8063153a59efce7f998dfbc2c56a293a866ce6f5f
bc353bbb74263bb0275dae7d6ba17b90620b01d99077a434cdc30718303e5970
0f8e77dc91fdef345a669aa4f2b19eb4367ee5269eb788ac08b9604bc2fdf427
579164bdbef2a53037a839f6063182b55d2e359e3dde2fe64faf96f04fad460d
7879d69a2c75ffcc5e6524baed51606398757b94e5d444b15f92ff0f5dd67ec1
b819af37e02b7833cd92d82e70768e8f98687b2d95d9e6f2205efe7039451e0f
f0424ae27e1c0737fc5ba2621ad892fdd1ba84dc2feacc74d05c03981143dacc
cded3a51d35855526f50b496a7ea8ba57414f80653c4655a3929b822ad2382ae
38d9e7c9bc8ada86b2dfc04998840d08501a4346107a08c944788ac20b38bf25
d7ec4eaa6707676107bd103fd4e0bdb89a92dd402d461513f0811dd8b1e41673
4b249f27e9d7491f19d2935f5628807e7ac424540572775c5900da3f8156ba10
2a26cbd8f2dba5807c1e8593a3b3f52da37df216ec929b59877f59336ec9778b
f5e259e45b3f925ab725c0fd5650d140090b2e1fe60a7f55e4b753d31be87643
06e8350d90bae8c2514750c69c5f5c1bcd728808b4a71e94a32ad5c0bc303e0d
bf6a75af429efabab84340263b9e20c99a12d9b59f215223a1b598da44f3d72b
8d201f1f5a9fbb139b3ff952d64128a6827a39b5f025458dbd5a5cb55c91fcbb
476a3068857d3307ebe7dc57f9fcd7772ce9afacd62153c58fe41542a4c4da61
2f84bccc40ce6735c137419c2ee251f70483197834121 2c29a4f844872af7a89
```

```
1f27d9a425522fb4ada33eb8e2e0277a1bc6cb83c32150467cc38fb4a2c89ce7
af20b812ddda83a3fea8d887b1c965b9c0406a7695423d75953cb5801e89229c
91cb57a93dc85a55965a772319dca8be32401c5d295180bb3833a1cf3f236ae7
fb45aa88e9ad406c8ef3ff59122c00c76601800be94bceff146d6e688a8bee09
5bb107692709681ed7ec7570adcf8edca68d4d046837100e0b8acd52ab5b47cb
a6342faaeb3bab04eda7ea9f543fc49e03952f3575c92f451dfb47d028abea01
f657e20fb711faf25b1cabe8f2f1af919400e2f87f70a6f2be3a4165f823cf19
4bd456297ebd5f381e4985f6e57d235703ca0ac933dfeec1d24f890f5518eabe
a487ccc8f9327fe1064df9a93cb0f5fd24bea2a34fd2722118730bfd9b0eb14b
922e53ebcee84f08eb71e99845f7bbc1b6e2dbc19b032c28116b8fbb7f1ffb74
2da5c0680116fe98312ad0f27d6d3251e70e1a6ae77fdc7bc2276f3a107f3e8d
01a08f101b3cd007a0d01a3e2c6e8fe94111375281e97da582f750baa44845f4
778ac180d6db2dd9e14a1693afa78371d1776eb566e9fd86995f47c84a48ffe4
e6ee1b22aa389e951362de97d8f79dbd1d1cba0bb21b031a8b1a9c1825703a19
4bbacc93411b94ad65440cd2cef14fd1b9e36dc01bd08d027ab059ee3ec1f8aa
da6285855e497db91225ace9a1118916d9c876e8c26c594f2dc058c49a398c66
1c030c9f0c1eb411e45794585cab438075f6b63b67112aaeab49e1c5b5ebe127
d933b9b0ece8736596f119b8999edbf0f2866aa4eecefde576fefcfcbb0d6cf9
0bffb2848038573169bfbb046b9e77c121f13201c4759d8da5deca8917a4dc05
eb6c81e85836113d20cac976394a96994556ef95c684aa817240217e0f5ad698
fdc70e09652c3c60500a83d5bf3192d107be5394ca9ab06bb13270574e61c892
b7ab9e3426036f6dd3035bf838b5c501ae63e58d8abb487bbdca4463bc040bce
2a3fbf776e34357aecd772a9b78aacd5d2679035ca07f79c4f89ed7d6beaab7e
44485c165cfbbc740c13efa8083726cdc58bf29437b3f3ae3cd747f8a6554e18
3d8a71d4d81d9a0b0ff4bd7034dc8c3d5e82c4435a81f49a9dca25af529013e5
745bbf7fa10740f9722ee04cb6a3baf64dd0733e19d15c3797f707542675b842
04bc3837994b39f5ddfb2ec488e64c3ce05a8e71a6b9a1ac0ac52b7f62c3aa4d
a4509403c5a2f9dbdab9c6ebd238c44d838cf3738df49863d33e265b47b3007b
28549cc49e7ad7af62340e60bfc9c341977fa9e201371c0aed14a5427b0cc825
0c914daea14f9e4407a6a8b3efb025acb9c3489e87712c5229f64696a3292ea4
1caa1fa38790c7a1967940ba86a2cdc328d3af0c5cafd5e1104e69299d36fa09
249fe84b4c9116081ce7197c9506e035750ec4e684567bdded18603136c5f683
109d2e3f21aa8f386760d65a30fdced79b10e3a3ad24a08b1ae255aeab9622de
6932708faeaea435702d03c9f2458547d1580745923321add7de174f4e991959
c29c3161e97f608bbb1521babb58d9cd95122c0d0f981ea957001b7a5d00a2c6
1e8fb6f8f88cb5c6d0c753811afedbd4714adac0ab5ba66d3dbd18aa1e25dad5
5ddd8be2bfb44f339093b88ee5bfa5f42578b3e757d5031cbc235f782e8dc47f
7bb0e70fe23a9b1bab367369a8c8943aefd2bf5d177d170bfb3b1914677c21af
809b183c8ef1d101539e81d68bfbe7b56f9440e34c5123fb1b4ca2a4f148cdba
b3dce1dae8c1ab6195f1212102853d82bbe02c2bb6a239593a7ff3442e347271
c6d1f24b6196aabe19be91279dae3f1a0999720af6b771f0481439ec08b2fa05
b0650dacf5150b444cb7e257b8478375d75eb79f6ff9c93eb37b38e0908c5a09
2aec53cf6da836ae5a02b9ce34053f7c3dc444782e820a90873b36c2f2c4e31a
4f2e7fe78cf96361b01134cec8a6cb27635749a24690ed1dc8528d0f43bb4ab6
40c9ee179a83f42bab07ee2c0a013c102e9427cfa15c0812d2d9c4109e545c19
1502d3ceb590b3a4de440282283a41415bc6665feb28da019fddfe25fc879bde
09e508e4a446bbf5330595280cded2fa52849a41010acf3f73ee83ad5e3bf576
7f1b6558b35d94332a4f5dbeaa19e078c70ea21dd9b65e852838dbf4e87e10a5
```

```
3d27e6995c7d649ca890021c80ff9b2ff3ee37fcedee25e06641f3af7a2c8167
696eb6b86aa648282418f2867733ce0ab435fcebe291d1d142373e8ba22504ae
26ccb2ace28080b212124d21a003a8bf97d5d130f8e8b305d3e642c8cbe50c21
add0441df5a2d2f6d1e1682a8e376fa2dbc28efae613d2da208bd71c14aeefa0
c366fa05876fa7bc0a64563b5c0388bc1c55a25f31a734fa7d36bfde38273e18
1415ecffab455c1ffecf8e1a1fa4562f5456f31935e2d494cb42815a0a08779d
8c3ad8f55f25b088746026b313a1365e60d2b5ee8d3ad0c6e2aa900a8f231db8
e7eb134d66a9e10c361ef53df8e94f99f2dd54d9247206d9795f35e439c31b92
e1cce1ba981889db7f3a74ba70f7a769fc4aeeba088cb5e5a587ae23f6c88f11
2577275dcb216aea650bbfee47d7ae61f03c65f9bbd6c8067854b5806ce5d9f0
f8a8a92ddc91f7011f2138b4029e68a9f7049f58b1ae61b9f61afdf47f43fb78
31069265df2d463a7b2929a49ffb65fa3bcc9948ce1cbfbe7a92a710cd567d90
15453cd9f8d31a35959adbafb36e4b56ef92858d548fdff47c9ad351af9548db
01d224ae587da5a1d741614cec3dceeaae04fb5c6ae08a49447db82dd15fd83f
eebfbc84ffd62753c3ab9982bb1acbfae08148839ba682f7042b239ff8b74266
a3a41774aedb16aa609d29ebc5b582dc7f8643ae72c74ef92cf63e1d6e787c3f
02ffafb377cb834c9bc60c42ae0304da0b3e4a530b6c358e9c33464b5143fae7
a8150919dcb51265c3031bb4e8ab8a1c11aacdc9d58b09a1f15c2163cf652799
d3254d3f4180328b893a375fff2967ebf9dcb37b70bf78db6b8262725865793f
296d5712424edec862557925cdf01dc5064c47009aac4d422de070517d483781
efe6c9582c50940e137daa24db2438006df3f2a3b0d68f7a540ef0e8197c3412
d99f94e7a1f92e8e3a00af9fc1f9a194bebedb3e045ea85ecc55df361fb8a152
c574d178816235c699b2058f57bef2ef437023a1bd0015d75e90a0f46c548e60
246272e1a6c2d585bd20437da4e98770a42e2c7d381bf7ae777cb60a84e5da8c
b51477df1a9931f78968faccca93b8a2c69b35ca0e97f0b535df4b383c221641
9a10683e11c93a4ddc5561448ca17c7ec3157c47867c8f5bf8a42d64d51e2ef9
d259b0b7663e96a8afe63b0f6b981bfe5bf314c0acb61d56fd4d4a98d9eeea79
80706bfde74108ea07bff67077d41b0954328b650fee243b9d7cc61e0510711b
5af93f21896884a11a3aa067a8fc4ea365bebabc98b0d72f35273210c6517e79
cdfabe419c354c9d6695c56fec9dbf27487ff33d0c24301d15619f536b315e17
1537667771bec78440eb25082bb91ca8c39d146359bf4d8ea18f85f33dc48aa4
faf5eb8579043cc9043cd175ef484b3ee4566bfa42a8a44c51c122ec5c00f84f
6ca6811943b8b525202b5fd5b41ba1ed711d68c953a81964db4858762d6522a3
c4409955cd55af15dbe2da77b1081dee755126018523efcd54e7ad62db7b6394
53da59211f4ebd3b6c1001da3e8d43664bae414a6b6c10e8c3a0ef6c992901eb
1450d50ebcbf7825eeb116fb0bee4bad16578f92376e3295aa9b556c65734809
1375d37c4b0ecc9d2f70102f55a41e0a2a5c08648b56d838d9c05f8c76d3c9c8
dd847c06f10dd0ccccf1d30afe0618a5caeef732f881139d7fb0f7b4e2ed826c
0035271f5f0cbeae956e8c80649a4e28dac72bfcadcb64122bc3f8006f2e45c6
89dd399954f3f59c842924a6ee4bfa2f3c47a15301131cbd4336de726b9cd47e
554a8a530b7def06542d123dafffe329c5690a95b4b0809a14c174d43d76cafb
e0818bf94dc89e400a8d1237709d93ce3ddd9e561c3c60b33189669796cfea60
7e41427a5466fe09ee526e243c648c34435b298047b8216f788a7e1593ff1fde
08099899713bb343626c505e2ea0ead112baf435b287fc20c43c80ed5a16d76f
b4c29a085d32baf72edf628466f7a1b797d0f3ddee8282c9bc5ffb35cc2c533f
127907434ccadf1028c653a1e026e95d913f53923745e173f43bf9bded089e79
8f5883b03e0dc47fc530f5784a95eaa880042c15f5b5f995421f38af6df9cd79
492d71e864113e9666ac091e2c41b3b73082425823faaf54dd3ce38ecb1289fa
```

```
  86176932dbffea4baafadd6dd9c4befa989d5a7758c7b292ab29c4b4cfa09253
  48b705a17cde3267482ca5dc80cd1ebb795c205a0de80f5de86e4fdb1bcb4a83
  d2133f936c3d936ac8853084697edc69ff1e0bbc9a06d585114c198054f02747
  a51715b1b1c6bec922b84f6d49695138fd7a55d3fc7d7ca399823e45710123f9
  7da50fa147eeb2e1c068113c83eccb9a6a2dc76f7b657182c08fbde037f0b843
  08838110e906f1fdae5157f17c6d86d9d33a4b6e3f3b65b83ec916eeb650c491
  bb5c5503c92d6172b5edc8e6011ac65230000013fe467033834c85c19944a0b7
  ee3babd1f56804bd32823c87dfe5694ea66d6275ca47a503584386fff0b3022b
  2d17d0683afa8cc19928b1ccc121d22ae055512e2a56216105454be55046b5b3
  4e16af1fed4ec63a60b247df336217139b4aceda6f23d1c0c47edb819267342a
  2e538b91a8d85e9c255a304b8612c85c40386cd042d04ea5b8e09000ad1b2a09
  96601813d2aa4de1dfd6026bd6186e7305ab31dcb9994e1aa39e40ff4c7f4e37
  212b5764c3976e3b9472bb46deb07359ec84e3b4e12efe0984ee40e785e8608a
  ac794f52157244fc85c88e2e092ef480a977196e9631f4ef242618574742c64c
  ce7c6addbac48bf339e0fb4882bbc775',
])
```

Figure 8: Example SLH-DSA-SHAKE-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