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

FN-DSA for JOSE and COSE
draft-ietf-cose-falcon-04

Abstract

This document specifies JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE) serializations for FFT (fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA), a Post-Quantum Cryptography (PQC) digital signature scheme defined in US NIST FIPS 206 (expected to be published in late 2026 early 2027).

It does not define new cryptographic primitives; rather, it specifies how existing FN-DSA mechanisms are serialized for use in JOSE and COSE. This document registers signature algorithms for JOSE and COSE, specifically FN-DSA-512 and FN-DSA-1024.

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

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-falcon.

Status of This Memo

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

This Internet-Draft will expire on 16 September 2026.

Copyright Notice

Table of Contents

1. Introduction 3
2. Terminology 4
3. The FN-DSA Algorithm Family 4
4. FN-DSA Keys 5
5. Security Considerations 5
  5.1. Pre-Hash and Hashing Considerations 5
  5.2. Validating Public Keys 6
  5.3. Side-Channel Attacks 6
  5.4. Randomness Considerations 7
6. IANA Considerations 7
  6.1. New COSE Algorithms 7
    6.1.1. FN-DSA-512 7
    6.1.2. FN-DSA-1024 7
  6.2. New JOSE Algorithms 8
    6.2.1. FN-DSA-512 8
    6.2.2. FN-DSA-1024 8
7. References 8
  7.1. Normative References 8
  7.2. Informative References 9
Appendix A. Examples 10

A.1. JOSE 10
A.1.1. Key Pair 10
A.1.2. JSON Web Signature 11
A.2. COSE 11
A.2.1. Key Pair 11
A.2.2. COSE Sign1 18
Acknowledgments 20
Contributors 20
Authors' Addresses 21

1. Introduction

This document specifies JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE) serializations for FFT (fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA), a Post-Quantum Cryptography (PQC) digital signature scheme defined in US NIST FIPS 206 (expected to be published in late 2026 early 2027).

FN-DSA (formerly known as Falcon) is a lattice-based digital signature scheme based on the GPV hash-and-sign framework [GPV08], instantiated over NTRU lattices with fast Fourier sampling techniques [DP16]. The core hard problem underlying FN-DSA is the SIS (Short Integer Solution) problem over NTRU lattices.

FN-DSA (formerly known as Falcon) is a digital signature algorithm based on lattice mathematics. It follows the hash-and-sign design introduced by Gentry, Peikert, and Vaikuntanathan [GPV08]. FN-DSA operates on NTRU lattices and uses fast Fourier techniques [DP16] to make signature generation compact and efficient. The security of the scheme relies on the hardness of solving certain lattice problems, in particular the Short Integer Solution (SIS) problem.

FN-DSA offers:

* Post-quantum security under the assumption that NTRU-SIS remains hard.

* Compactness in key and signature size.

* Efficient operations (roughly O(n log n)).

* A requirement for careful implementation to avoid side-channel leakage (notably Gaussian sampling must be constant-time where applicable).

The sizes of public key, private key, and signature for the parameter sets are the same as in the original Falcon specification:

Parameter Set	Signature size (bytes)	Public Key size (bytes)	Private Key size (bytes)
FN-DSA-512	666	897	1281
FN-DSA-1024	1280	1793	2305

Table 1: Key Sizes for FN-DSA

For a detailed comparison of FN-DSA with ML-DSA [USNIST.FIPS.204] and SLH-DSA [USNIST.FIPS.205] see Section 11.3 of [I-D.draft-ietf-pquip-pqc-engineers].

This document defines how FN-DSA is used with JSON Object Signing and Encryption (JOSE) [RFC7515] and CBOR Object Signing and Encryption (COSE) [RFC9052] [RFC9053].

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 FN-DSA Algorithm Family

The FN-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
FN-DSA-512	FN-DSA-512	FN-DSA with parameter set 512
FN-DSA-1024	FN-DSA-1024	FN-DSA with parameter set 1024

Table 2: JOSE Algorithms for FN-DSA

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

Name	alg	Description
FN-DSA-512	TBD1 (-54)	CBOR Object Signing Algorithm for FALCON512
FN-DSA-1024	TBD2 (-55)	CBOR Object Signing Algorithm for FALCON1024

Table 3: COSE Algorithms for FN-DSA

4. FN-DSA Keys

The FN-DSA Algorithm Family uses the Algorithm Key Pair (AKP) key type, as defined in Section 3 of [I-D.draft-ietf-cose-dilithium].

The specific algorithms for FN-DSA, such as FALCON512 and FALCON1024, are defined in this document and are used in the alg value of an AKP key representation to specify the corresponding algorithm.

Thumbprints for FN-DSA keys are computed according to the process described in Section 6 of [I-D.draft-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 FN-DSA is beyond the scope of this specification; see [USNIST.FIPS.206] for additional details.

5.1. Pre-Hash and Hashing Considerations

FN-DSA, as specified in [USNIST.FIPS.206], supports both pure and pre-hash modes. This document specifies only the pure mode of FN-DSA for use with JOSE and COSE.

This document does not define or register separate HashFN-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 FN-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 FN-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 FN-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 HashFN-DSA could be defined in a future specification.

5.2. Validating Public Keys

Public keys SHOULD be validated before use (e.g., against encoding constraints).

When an AKP algorithm requires or encourages that a key be validated before being used, all algorithm-related key parameters MUST be validated. For FN-DSA public keys, this includes, at a minimum:

* Implementations MUST ensure that alg matches the intended algorithm variant.

* The key representation MUST be of the AKP key type and MUST contain the public key value (pub for JWK, label -1 for COSE_Key).

* The decoded public key value MUST have the expected length for the selected algorithm variant (see Table 1).

Public keys that fail these checks MUST be rejected.

5.3. Side-Channel Attacks

Implementers should follow best practices to mitigate timing, cache, and power side channels, such as:

* Using constant-time arithmetic

* Maintaining uniform memory access patterns

* Avoiding data-dependent branching or memory indexing

5.4. Randomness Considerations

All required randomness (e.g. for signature generation) MUST be derived from a cryptographically secure, high-entropy source.

6. IANA Considerations

6.1. New COSE Algorithms

IANA is requested to add the following entries to the COSE Algorithms Registry. The following completed registration templates are provided as described in [RFC9053] and [RFC9054].

6.1.1. FN-DSA-512

* Name: FN-DSA-512

* Value: TBD1 (requested assignment -54)

* Description: CBOR Object Signing Algorithm for FALCON512

* Capabilities: [kty]

* Change Controller: IETF

* Reference: RFC XXXX

* Recommended: Yes

6.1.2. FN-DSA-1024

* Name: FN-DSA-1024

* Value: TBD2 (requested assignment -55)

* Description: CBOR Object Signing Algorithm for FALCON1024

* 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. FN-DSA-512

* Algorithm Name: FN-DSA-512
* Algorithm Description: FN-DSA-512 as described in US NIST FIPS 206.
* Algorithm Usage Location(s): alg
* JOSE Implementation Requirements: Optional
* Change Controller: IETF
* Specification Document(s): RFC XXXX
* Algorithm Analysis Documents(s): [USNIST.FIPS.206]

6.2.2. FN-DSA-1024

* Algorithm Name: FN-DSA-1024
* Algorithm Description: FN-DSA-1024 as described in US NIST FIPS 206.
* Algorithm Usage Location(s): alg
* JOSE Implementation Requirements: Optional
* Change Controller: IETF
* Specification Document(s): RFC XXXX
* Algorithm Analysis Documents(s): [USNIST.FIPS.206]

7. References

7.1. Normative References

[I-D.draft-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>.

[USNIST.FIPS.206]
"Fast Fourier Transform over NTRU-Lattice-Based Digital Signature Algorithm", n.d., <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>.

7.2. Informative References

[DP16] Ducas, L. and T. Prest, "Fast Fourier Orthogonalization", Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation (ISSAC '16), pp. 191198 , 2016, <https://doi.org/10.1145/2930889.2930923>.

[GPV08] Gentry, C., Peikert, C., and V. Vaikuntanathan, "Trapdoors for Hard Lattices and New Cryptographic Constructions", Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC '08), pp. 197206 , 2008, <https://doi.org/10.1145/1374376.1374407>.

[I-D.draft-ietf-pquip-pqc-engineers] Banerjee, A., Reddy.K, T., Schoinianakis, D., Hollebeek, T., and M. Ounsworth, "Post-Quantum Cryptography for Engineers", Work in Progress, Internet-Draft, draft-ietf-pquip-pqc-engineers-14, 25 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-14>.

[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>.

[USNIST.FIPS.204] "Module-Lattice-Based Digital Signature Standard", n.d., <https://doi.org/10.6028/NIST.FIPS.204>.

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

Appendix A. Examples

A.1. JOSE

A.1.1. Key Pair

```
{
  "kty": "AKP",
  "alg": "FN-DSA-512",
  "pub": "V53SIdVF...uvw2nuCQ",
  "priv": "V53SIdVF...cDKLbsBY"
}
```

Figure 1: Example FN-DSA-512 Private JSON Web Key

```
{
  "kty": "AKP",
  "alg": "FN-DSA-512",
  "pub": "V53SIdVF...uvw2nuCQ"
}
```

Figure 2: Example FN-DSA-512 Public JSON Web Key

A.1.2. JSON Web Signature

```
{
  "kid: "clpwZ...RWYU9CUF",
  "alg": "FN-DSA-512",
  "typ": "JWT"
}
```

Figure 3: Example FN-DSA-512 Decoded Protected Header for a JSON Web Signature

A.2. COSE

A.2.1. Key Pair

```
{
  / kty AKP        / 1: 7,
  / alg FN-DSA-512 / 3: -54,
  / kid            / 2: h'66616c636f6e2d6b6964',
  / public key     / -1:
h'09098e1e15e457c27018e854a4e4d53c9a4067ab03cb6a698d7667177a85905a
  d33dcd443799bd8ab6e20770c17840aede1ebecdc125beadaa7f22e880fc9a58
  0b61086997199774bacac649ed342d75355a23e44c48512500688b21684edf76
  ef4c7d78d024737fe100290ce8530fcb46a6546d295152df960438f71a139917
  fdf5296322a5bcdafd2a468c74470ee3589a9f9a2a5597436f50fb1a2a93e27c
  c4f1af290f38cc017461c85b8996d5977781ef37330f015cdd4e293b9a6995a4
  2d254bdbc71fdddebb0886d9148216b2b2e147a5e87e58275ec9a05d9b916aac
  c3069ace28c144ae4b529288eae34a2b4013e240c1866de591897e1d3e75e8ca
  997d612f329c260ace6d4d1e32e2cad0e41f0271af4532922a904622d2a255d7
  82b6225aa1249a4499b9f5a12ad219f90ed5a0d0d6110de9d417a5ba8e656524
  bc229827e0e8694fc96e8ad8aea052a32458790e53d041fb12dcc1c075e6dc36
```

```
    0aac84cc2f557ae9e0ab676c8c0620a383a12ec189cc2af5414828773881f5ad
    ef9c81ac5aa2492a26a7007a7b12adca1f3c7866735b0204885c38d3862a298d
    2f1777a961062eab1a9dd2d15a3970915849610ee5a1c1e7882a2c492d753d1e
    8569d883a0dbe3509a7dd142692fe143253932ec9357aa5c11fb0c07aab12cc6
    31c8e0b13655c26acfa65b4cc220eb4bcfab397434eb59402c227a6e7173ea00
    79485838d00d265f04de72a196af79bd281366dea227755d2a2c03c26f9ebac3
    ff4c3b490ce857bd1cffa2a9ef960def4f8179f75b6f2ad820b9a754cfdfa379
    5e4524c203710b099008c85e194131bba0d304c79005cb08f5c7dd188662488b
    cb02acfc1a5b554dd3bc36b2d176dd0bbe2678d37e065c52e279c58142959941
    f1a40f045c879843f2ab8087467c1745f1e2fc74ea31d710ccb19fcaa0644c8a
    e5bba4a3e024ae84809164eaab0ed536e2c2e5fa4511b000b42aff628e236d56
    e4b4c80b744892157cd567302cb049cde1087b38189aeacf397cf04fe6c70b3d
    5b1caf92bfe6097f88875abcebf45b1a30b3a58ce61e9c3abb528be07a94b7b6
    355afe6acdd39838079848b57d1984d0efb574bb62844a872f39d065e6ea2b84
    fe6d855dea568c5cfd45560c89389816a1b947419276ec21ee8a9e39ea95e725
    13b94b32a5c55e185b2eec1255671004b9825e7947de3756ad5515396cbc732d
    aa97a9e5bd525901fb3718d47a22060b80df8ca559a8368a92008269b69afc95
    e9',
    / private key    / -2:
  h'59ebc07f0841ff04803c103078f061bdf0207cf7cec4ffbf80f4407e002f02f8
    0ffafc408310507e040ec30fef7bf3a0bd0c3ebc0401c1fbdf7b083fc0083f87
    f8303c0fc084f84045ec2086d031c3ffa08808af4000418cf3f1fef00ffaf830
    43f7fe83f8213bfc2f84fbb0fc1430fe0c7f01fc2f03e0613b00407fefbeb82b
    e0c1181fff03ff00105fbf1bff8407e08014117f00227b2bdf8307ef81241f43
    f030fdff813ae010faf880fe03febeff70bc23f138ffe14407e0840c0f41ffef
    bafbfffdf3f04504003a20bfc5f03f45084f3ffbc0fb180001ec6ffaf070051c
    30c50c313b145ebbffee3f281ffc0431be17d17ff05e43f86f8727903c17c07f
    084f7b180dfcf40efe000000ffdf462fffb913a0c80400c60820befc7ebb044f
    fc083f000bbfffec407cf3b1800fd000f000ff089e40104eb804514627cffee8
    5ec1fc5000fbe18208600807e1f8279005fff001ffff820c117d18004104203f
    140f06ec5d80083fc1079142ffff86103ec2efc03dec303c045f7fe44085f7f1
    85fbd10327d043f0203f1001befbb2020bcfbcfbe1080fcfc6f3e044e86f81fb
    ffc1039f7dff71bf0071c3fbb2fdffd17f0c3eff0fd0f6e830fcec0fc0104082
    f4224607df07084044ec00c1ffd183040040f84fff084fc2f83081ebe142f42e
    84040081f40f84044e000fd17ffbe0fb10507de3df03ebf0bd03cffcebf1000f
    d20117d23bffee05ec607c0041c00bafbcf400c3fbffba047001f7dec20bcf02
    f3ef7c17dffbf831befc02841430bd0060c200217d200001f46146f40f3ef8af
    7efc2f050fbff9f7d0fdf8004907af41fbf001f7b0c5001f02e440bf1811b603
    d07ff830c3c7cf460391bf14008107aec4040fbe03ff02100ec404403f0fbf40
    1821b8f410bf080005045f830040c0f410be03ef44d841c6e0100017ef3effbf
    c400413d13f2fb0c2000f80fbff840ffffdffe0bffbfd88f7c007e84e3c1c404
    407dfc10430fc1fefff048ffc141140f8603d1c7f0508107b0bcfbf00113cf41
    042ff818a00223be3ff05082ec1f3b080fc0041e7ffbf083e461ba179ebff81f
    3ddf0d0a14120ee7071fccf901e606e62effcf0b1e00f805190fe71a1600ddf3
    131503f00fe4f9eb2bfbe537020eef0e15fefa0f4015f9d8ebeedad402f1ede1
    180730020ae0f603ecf808dcf801ec0cc5c2f3f40cf0c9e9e31f24f201f6e5d3
    2310d90ae5edf9fe101fcce8bc20ca291d092fcb11e811c10801f41add41e932
    362af2d72aeaec0317020f120e18001c2be7010fecf9fac829f0e9170b42f315
```

```
    25ed29c22c14cb240aeded0ad8ffcdf0f7ef0be1f211f705e4d20ee51025f5eb
    0ddaf116f8eee31d26ac1c05bcc5e119dec9ddf9200121bf28182416341db313
    2ee6eaf90af3fedd08f90e25eb0dd90df0eb32dc08fe0a1ff90cf1fedc2ad31e
    31fa0f1a01ed071a08f8191a0de2d5edc114c309dd04e92b08cefc37f63dbb26
    30fcee2801f2d7dd07eadff1dd0af917e8f7ed060107f5b93fc2f7f406efe928
    ded9063329f6f7171ae31de6e31ae3050cdff5f3fdf30f39d3e2d12f33f5c32a
    1535f5401ef203f1fbb0fc1304e4e3ee01fee9fadbffc8dd1fe94106fa35f62a
    11e5f709ebda26fa1ecd43fce126df08d8150c06f7fd17f91bd20eda1d0cf208
    f4d40f2e01e6b822f202252303caf0e32cfa0fd9fdede3ff1bf6dbe810ea20eb
    0916ec1d111a0b0526db2a3a14e50012f3f1c72c140fff0625c71210fef91202
    f20efe2cf7fb0011f0cd03fb05ec0509dedee731dce12e2f25e50030f515fbd7
    d4'
  }
```

Figure 4: Example FN-DSA-512 Private COSE Key

```
  {
    / kty AKP        / 1: 7,
    / alg FN-DSA-1024 / 3: -55,
    / kid            / 2: h'66616c636f6e313032342d6b6964',
    / public key     / -1:
  h'0a81ad206a1c49a981cafbb70f15c6bec2b033e468488518b388088172142cf1
    5094e85dab1a8534d28c0e72fc7df5126b45536a9914729542837067586d408e
    56146ea99ceb5391421f6a3f198143dcbd18234f74bb0487c53e2a6530fce990
    a40fd42c7251c52f0ec34f5887e9799d0d76f0b978b109a6af287ff2ce20a7bf
    24d825a0dcae3566b163e5da8843b1b748360a405822c945811364021d757687
    2c75507200781ec2b992b1feaa6564c5a2647bb962c34e55c057a3c141ab7e78
    253a26ebba4fd8c81a2842f89fb1ce29f328769302f4c91ca02499b165478fac
    4262ae89747126904051aab678133e0d892ee77966cc2b655ee376e3437861bd
    345c14ec202d68004ae1bc86d8527a1b9f6457862d1465e3910d1cde3528e2ea
    4d211871bea7b79c0036e0accfe515d1afa5cee5d9b2ca52b839a63c48945a70
    078a8e2e6a80d910a326ad06e4dac7103a47d4c4b9331df9af98575a03876d45
    42e85372c5b45321ef75c682c26bedcce778d9181e257179435a9c801eb19bf6
    8bdfafe8a10b4d8faa9d3522388b6cad22d511c46490ff1d38bcaadd548b67a4
    f1b9f922c7852a137150cc8385e18fe18a02f8b8aae2f705236132d8d2d2098e
    b61032a5b7edd9583422c607eb21f3489cb1f91a5101575a849bd56d29628654
    d0268f451bfa73742952456c206c693a240051b19ed92892ad3bee0ad3d0c040
    11eeef769b85f09b6a6386bfe3c325ce0d1ba26eea3e9e9d42891a6ca2342da3
    5457632878c0c798175f4f366ec48a4ab3633ce1d6a2e81384c6db63d48fb736
    bcd037accbf758422cf43409b747a15e7baa8d8911f529e60345fd1452a2260b
    18f50e2513593c02134421e470cf58e875c48100bc2301569dd90b901eaf7e64
    b63b6be7b22a658e735c1bb380add1f0f1db136f899448cce33092b8d4f88390
    65710ac9231a0a2684f113c4ed15de0d7d3ee43d57a7b969cdc2394a0e99cd99
    f6cb62e66125a306c70c4d577d07cb7b6e3a666103767167fd3d9ad1a538ecf2
    766e99980a82af5e30c6916088d6109cd2c188e61094060a04d0ab841b6825d0
    a8c86109621fabb86d8731927d54fc51b5885d3457e602139fda423a9ed1c8bd
    69ccc5b3d7672514f557c7e884acd834d3b3198063e6d201ac90075e099841af
    eab96fd513e61481350a49bf86e6d20d7ccdf3511e437dbbad7884bb9a259c01
```

```
    335a580ec2bd618c4163975fab349a53db6160ab20e691324ac275b11c6302dd
    3977a9fc3a0f68a59cc6ff21b9c2dc7eb0600395e7689069978bdd2a0b3f760b
    07180f5a24004d382f91d9b32808a9d4d9038f89569be86df0926da176288d1a
    1a2e38681edeb217358be30fd15b48fa6c9bd6deb87aa40170d086256660e684
    64ed0575940f872cc5c2b2e8162afcd0e3bc1c9e6248c0f152093282459c0d55
    4624085d4882a4f2313ac7e8c8baae39e2dce589879d2d88921f7d092eb317b3
    53652c0a7d6a7ed97f3cc8ec766045e6bce4ebe409920d4ca48f4648e131b2f1
    ff0b374a5e6768cd494e1e5d86786896b1ae1e0e1000f05b51e51a9c4cf0b3a9
    bfb1da29377bab94b30db629730e2712b1d405c7dfa71e9a55880feb121c145a
    0a08d81954302c66dec1893342c0110dad1fb5296c54b0d84e29dce8c80e4751
    006174d3e256391b48efc59f42ed800d37a397024891c64a400f62fb38a60763
    a99ae5528e0b686403eaa33285ca14901f6e0957136c1b7d8d4531c986612eb2
    3d2a3a346b1b173cdfd4eacaf42e41bce8a3d805a2bc296674c9f66bc51e27f7
    53028a406633c529b476097046ccece6826ab491c6e5791ed2fb8a3355bc5951
    5be3b3169bb8f17e46fdcae765f6dc32e707b849b9b76ab4804690d2cb102086
    af1ded9820aacae86ff6e8306f630d951c31b9eb543a8fb46b85b7a0d26c5227
    8813da6563a58635e06926530885c53c2df9ba4223c7faec148e5e3f227ace46
    655e7025406f08ae98eea2b1d1aa80213b8370281c5474d386795bd78ef4f204
    aa8a736b1662a3f65cf4b47c3f203d698a47a82aea11ce04a6e223358f63c960
    ea4241f7a5c8631689654653912c7654473962d688469c97381526315203e0a0
    5d4c3e0ec3899a107f75a53ecb7654ac318c93dae4af082e79bcebcbd59b859c
    e9e31490f65b150ca1e8d39498a432f3e6954b0b6e41b150ddc532a86ddb5300
    5431905d05ea6324a976d0ba0846360b2e8e16811cbb7ebd19e08aa12e4c1480
    5a36853ea72db2e419681036feb1f6d76d35b69a236bfd0b069e561f26fd57e5
    b9eee1b6d44dac1eace4d20ed82c6c269663e544e61f119c8087aaf50ab9b546
    68274c64a1ebe1abc2273ce56e199dc615b3787f28e39e59a9a9fe9409da0620
    90dda41805628f6d73a9ff4dba77ca2ca9ee038041bd673274e93963b1cb87e7
    0ab593c899b1f14d862f7d95c1fc8bd91f60eef4c355fb070d45c77fe3051258
    572aab151f64be37ebf2605118b56a657281373b91faf14bd1a5ac7632e07a10
    74',
    / private key    / -2:
  h'5a083c1ef43e374422e3fde78c3e0fe33005b088450781c07c1fefc05073c50f
    3dfdf7c0f82fcf83e307c221ffbc0f81de87dcd0bbd013a1e8882113ffe889ef
    8c5f077a31a86238c3e183bfff7bbf8801fffdd08426dfc82f73c20043f0f3dc
    e701cff3ff2780410ba207fe30043ee8cc10fc1de787f203dc1106000401ffc4
    00900017423203642081e10404f0060f047d40be20f79d1039e0f424f001d213
    fee97e41e03f1044637c25ef40100440f77f9f0c58077c5077e116c80f843e08
    c230f44117b80d93fd1ffbef7443f8c01f0c000fbe00042410be20ff7c0f881d
    8fc510be02043c197a22003de0fa20846009005f83bff9022100221ffc000f9e
    f6c3cf07e51ffa4f90be20c2008c9b0f05c003e4ffba5183c3ffbde1f85effcb
    e183e0e7cbfe046117bc018020e6fe6e77c4f87be0a3e100c201f05f17bfddfc
    a2efbe4d8fe6e081f0005e1079e007ff0fffd00020ff3a1f03e128c0110c0007
    c62f8fe220025ff4030939f10446f0bbd183df003fe00be1003da1fbff0fc3d0
    9840e885cf9c051fbddefc1f1f83c190a11781f07fc11845e16fe0e9500103a2
    f78231f847003980885cf07a208ba20f47dd879c077c4e885fe109f283a1113f
    d008c011c00fff81f8024f8fa01043f403df1f422f845d25fa5e83c2193e0f8c
    4210c5ff87c3073c011764f108008c3b183fe17ffb28fc63f45c00efde702110
    042f0023e8bc5f743e10820283e0e00040ffc1eff7ff883ee7401f8c63f74def
```

```
efd9d83e0280000fc1bf8c40f08003803f3fb7f1701b28bdcf83e0d844119422
17c1f20bfbdf040e8fe51fc00ef403097bd0003f08843d8822fff810e4c31805
f103bffffc030ffd303c0177c3f03c2200bbe801df742007c9ee13bef133f007
e5110035f3dee04bdf03bc0f8201f83d10c1e07041ff82110c2218443df8c120
c3e2001feefa3efc3e28400eefbdff861000a5f1061090a4ff083f033e0f4010
8ffe0e802fef420fbe1e804037f62f089eef85f0f0bdc005ce901f0fc22173e2
f84a10f7de17c3e0883f0880201003f13fff915e1001d18c00e03fef0022f83c
300cc20ffffef77df709f26ffc1fc5e00484004231840017fde0787c21bc0ff8
220f0640003f0fc42190e7ef43f08f3f0fba7073c5003620845def444df3fd19
43ff7b61f1401f6fe0080641fbe30749ef6ffdf801f013811fc2008bbd16c24e
7c60e07e3f07df0efc208421f786230041093de0040300400ef804f1760f83ff
d693bf0cbbf0385f043ff7c3f07be02906100805d045f02060ef81bf04c3f8fb
ee8403c80020f002f785f104001f3e217bc7e005effb83f8442e78c22f041088
9ff13a52803b07c03f7c1e0f7bff8c3d47c410803f017a4ef404e0fa20ff7de0
80520360184bf47383f8b9d083fc0f3c0f87e0f87e0e78a200840ef881e14611
7c20f97c3f801df7fe0b0042fffdc17bc0170232700308ba10fffff8c1f28bc3
08c3ff0ba11900308f602840117ffc17f9eef46427c7b173fbf78de2007f1f40
1e8c00f87bff005f174830ffffd0360f14c0e83e0f8363f680221f7c087de070
5f107641f3bb18b2326f43f9be1ff81e1003e0081d107dfd07e0ff7e43902207
f7d27fc1ef8620fbe3f878408bfe08002087b91ff2006bc3f876010bde10d5cf
744127c64283a300847f07ddf0b410843c08be2117c4297bc0079ce849d18040
00c61f83a0efbe4073c40078237be1e70c0d8bbe31ba41f460d97df003c400ba
5f7bded804308ba0080410ffbe3f0a410001083a1ff7e4e6b41f087ee7bfc110
3df4060ffd0fe1fa0dfe1903f3ff10f41c0cfa150304e10703dfebf7e4f0df00
24f22f14341be3e4ea1a021b0cfefcf5fa03ebe123e711060e021eed0a1619e8
e4e8111ce20738f8feea00e5fddfeb19f4d2fb23cf2afcfed8e8232310141112
fdfcc8dbd8e51af737f0e10ce6ec47350d14ec0dd508e012f225ecf900f6e10b
f31e08c5f3351e03190e02f4fbf7ef06ebf7e9c228e00f092c1a2421eef2e711
1304fe2f1cf8ede128e8e7fb0f16e202f51b0516270148fcfcf729f9f122e8fc
1f071ce6d92418210232f6f32c0816411ee8fbee21f30818ef0e1310d527dbe1
dffc0bf0e624d51020cae8f107e7fee62c3cc5f7f8e3dbcddb2dfc1403160d46
edf822212ff0d0dfd4d4eaf009f9e915d1f0f80f1d141b35da072bf2f9e80517
0213e1eeb3f4e9ee19f0fd3124da31df02ffdfd1dcce06dff7080a04fdcfef0b
28ef00e9f402f4cd0a0bfb0d26fef5f1e31d0401143ac9ec16e016051cf5f5fb
dbe705051810ee2413000f131507ef01f50701ef3d1b0f0ff1ff0600e20d0b24
09f309e3f9e9f41a11fbdae00fdfeae6e40bc6dde5e30517dce413daff491915
150dffe5deebe1d108fbe9fdfef20fd1ed0339f51521fa03cb20022afc15ef14
04e6f1f10401e533f5e921040d0223f3f5efe0061bd9f308e801f7fcfbec0106
e5e1e232ee131709d40fe409d9dd1fda14081b040101fee40ef601dc21fc0ce5
e2fc362c051bf1d018e7f40a0e1bf2000d1a02270403130300ed0019f1f1d927
f3e1dfd9220deed8220ed9061a050bf3fa210cef20f2ede42506240d1dde031a
180a12f7fa322807e91f0c06b4fe22dd09361dce010004f7031107cd1633e0e2
fdfd030e10d53207f60e0bf6fde737ed0607ffdff9e0f605cd07ee2bfbe6edea
ebef081311e52d0114edff1a182affe102ffe0f42800f01719f8d5f3eec7fa07
0ef922eef1221e08fe1109efe80108d3c702d5eb12f6f007f825eae01b1310e7
12e4eff3080603e1030fdfe2d5e00530f31af6000c1d0bfb061eed10ff01de0b
0b220c27f0f0f5e923fc0eeff42417f524cf00e4d4f3dced06ef06feee280d2c
fb1326fcde1021db09d710f518f9daefec07e1c734230f11fa2e11fcfff4d5f9
```

```
    ff2a10dde2e5eff0fcd509ede0e9ccdfe60306050df90ef6f9e311231d08ffd8
    f8e6f2fb03ee160cf80fae1714f9d630e812ff16f1f4e3f30ad0ef1dc50003d1
    e9f214db170a0ef9f6ee140d19fded02e505f209fcf9130710032eeddff73428
    00291106eef2f7390df00ed81ef3c6f407f335f8eef60d1dfb24f5d53806040d
    31251eec1e200ce0e1151edf10e9e425fd04efeff306dbf704121b05052818f0
    f4f309f7fd1303050bfdf61831ea0f34f731ee04ebe5effd091a310dddeb2518
    d7310ae80b0de601e7bcdce91f28faebcc0cdffae10816280ad9f3fcd51b01d2
    11'
  }
```

Figure 5: Example FN-DSA-1024 Private COSE Key

```
  {
    / kty AKP         / 1: 7,
    / alg FN-DSA-512  / 3: -54,
    / kid             / 2: h'66616c636f6e2d6b6964',
    / public key      / -1:
  h'09098e1e15e457c27018e854a4e4d53c9a4067ab03cb6a698d7667177a85905a
    d33dcd443799bd8ab6e20770c17840aede1ebecdc125beadaa7f22e880fc9a58
    0b61086997199774bacac649ed342d75355a23e44c48512500688b21684edf76
    ef4c7d78d024737fe100290ce8530fcb46a6546d295152df960438f71a139917
    fdf5296322a5bcdafd2a468c74470ee3589a9f9a2a5597436f50fb1a2a93e27c
    c4f1af290f38cc017461c85b8996d5977781ef37330f015cdd4e293b9a6995a4
    2d254bdbc71fdddebb0886d9148216b2b2e147a5e87e58275ec9a05d9b916aac
    c3069ace28c144ae4b529288eae34a2b4013e240c1866de591897e1d3e75e8ca
    997d612f329c260ace6d4d1e32e2cad0e41f0271af4532922a904622d2a255d7
    82b6225aa1249a4499b9f5a12ad219f90ed5a0d0d6110de9d417a5ba8e656524
    bc229827e0e8694fc96e8ad8aea052a32458790e53d041fb12dcc1c075e6dc36
    0aac84cc2f557ae9e0ab676c8c0620a383a12ec189cc2af5414828773881f5ad
    ef9c81ac5aa2492a26a7007a7b12adca1f3c7866735b0204885c38d3862a298d
    2f1777a961062eab1a9dd2d15a3970915849610ee5a1c1e7882a2c492d753d1e
    8569d883a0dbe3509a7dd142692fe143253932ec9357aa5c11fb0c07aab12cc6
    31c8e0b13655c26acfa65b4cc220eb4bcfab397434eb59402c227a6e7173ea00
    79485838d00d265f04de72a196af79bd281366dea227755d2a2c03c26f9ebac3
    ff4c3b490ce857bd1cffa2a9ef960def4f8179f75b6f2ad820b9a754cfdfa379
    5e4524c203710b099008c85e194131bba0d304c79005cb08f5c7dd188662488b
    cb02acfc1a5b554dd3bc36b2d176dd0bbe2678d37e065c52e279c58142959941
    f1a40f045c879843f2ab8087467c1745f1e2fc74ea31d710ccb19fcaa0644c8a
    e5bba4a3e024ae84809164eaab0ed536e2c2e5fa4511b000b42aff628e236d56
    e4b4c80b744892157cd567302cb049cde1087b38189aeacf397cf04fe6c70b3d
    5b1caf92bfe6097f88875abcebf45b1a30b3a58ce61e9c3abb528be07a94b7b6
    355afe6acdd39838079848b57d1984d0efb574bb62844a872f39d065e6ea2b84
    fe6d855dea568c5cfd45560c89389816a1b947419276ec21ee8a9e39ea95e725
    13b94b32a5c55e185b2eec1255671004b9825e7947de3756ad5515396cbc732d
    aa97a9e5bd525901fb3718d47a22060b80df8ca559a8368a92008269b69afc95
    e9',
  }
```

Figure 6: Example FN-DSA-512 Public COSE Key

```
{
  / kty AKP         / 1: 7,
  / alg FN-DSA-1024 / 3: -55,
  / kid             / 2: h'66616c636f6e313032342d6b6964',
  / public key      / -1:
h'0a81ad206a1c49a981cafbb70f15c6bec2b033e468488518b388088172142cf1
  5094e85dab1a8534d28c0e72fc7df5126b45536a9914729542837067586d408e
  56146ea99ceb5391421f6a3f198143dcbd18234f74bb0487c53e2a6530fce990
  a40fd42c7251c52f0ec34f5887e9799d0d76f0b978b109a6af287ff2ce20a7bf
  24d825a0dcae3566b163e5da8843b1b748360a405822c945811364021d757687
  2c75507200781ec2b992b1feaa6564c5a2647bb962c34e55c057a3c141ab7e78
  253a26ebba4fd8c81a2842f89fb1ce29f328769302f4c91ca02499b165478fac
  4262ae89747126904051aab678133e0d892ee77966cc2b655ee376e3437861bd
  345c14ec202d68004ae1bc86d8527a1b9f6457862d1465e3910d1cde3528e2ea
  4d211871bea7b79c0036e0accfe515d1afa5cee5d9b2ca52b839a63c48945a70
  078a8e2e6a80d910a326ad06e4dac7103a47d4c4b9331df9af98575a03876d45
  42e85372c5b45321ef75c682c26bedcce778d9181e257179435a9c801eb19bf6
  8bdfafe8a10b4d8faa9d3522388b6cad22d511c46490ff1d38bcaadd548b67a4
  f1b9f922c7852a137150cc8385e18fe18a02f8b8aae2f705236132d8d2d2098e
  b61032a5b7edd9583422c607eb21f3489cb1f91a5101575a849bd56d29628654
  d0268f451bfa73742952456c206c693a240051b19ed92892ad3bee0ad3d0c040
  11eeef769b85f09b6a6386bfe3c325ce0d1ba26eea3e9e9d42891a6ca2342da3
  5457632878c0c798175f4f366ec48a4ab3633ce1d6a2e81384c6db63d48fb736
  bcd037accbf758422cf43409b747a15e7baa8d8911f529e60345fd1452a2260b
  18f50e2513593c02134421e470cf58e875c48100bc2301569dd90b901eaf7e64
  b63b6be7b22a658e735c1bb380add1f0f1db136f899448cce33092b8d4f88390
  65710ac9231a0a2684f113c4ed15de0d7d3ee43d57a7b969cdc2394a0e99cd99
  f6cb62e66125a306c70c4d577d07cb7b6e3a666103767167fd3d9ad1a538ecf2
  766e99980a82af5e30c6916088d6109cd2c188e61094060a04d0ab841b6825d0
  a8c86109621fabb86d8731927d54fc51b5885d3457e602139fda423a9ed1c8bd
  69ccc5b3d7672514f557c7e884acd834d3b3198063e6d201ac90075e099841af
  eab96fd513e61481350a49bf86e6d20d7ccdf3511e437dbbad7884bb9a259c01
  335a580ec2bd618c4163975fab349a53db6160ab20e691324ac275b11c6302dd
  3977a9fc3a0f68a59cc6ff21b9c2dc7eb0600395e7689069978bdd2a0b3f760b
  07180f5a24004d382f91d9b32808a9d4d9038f89569be86df0926da176288d1a
  1a2e38681edeb217358be30fd15b48fa6c9bd6deb87aa40170d086256660e684
  64ed0575940f872cc5c2b2e8162afcd0e3bc1c9e6248c0f152093282459c0d55
  4624085d4882a4f2313ac7e8c8baae39e2dce589879d2d88921f7d092eb317b3
  53652c0a7d6a7ed97f3cc8ec766045e6bce4ebe409920d4ca48f4648e131b2f1
  ff0b374a5e6768cd494e1e5d86786896b1ae1e0e1000f05b51e51a9c4cf0b3a9
  bfb1da29377bab94b30db629730e2712b1d405c7dfa71e9a55880feb121c145a
  0a08d81954302c66dec1893342c0110dad1fb5296c54b0d84e29dce8c80e4751
  006174d3e256391b48efc59f42ed800d37a397024891c64a400f62fb38a60763
  a99ae5528e0b686403eaa33285ca14901f6e0957136c1b7d8d4531c986612eb2
  3d2a3a346b1b173cdfd4eacaf42e41bce8a3d805a2bc296674c9f66bc51e27f7
  53028a406633c529b476097046ccece6826ab491c6e5791ed2fb8a3355bc5951
```

```
    5be3b3169bb8f17e46fdcae765f6dc32e707b849b9b76ab4804690d2cb102086
    af1ded9820aacae86ff6e8306f630d951c31b9eb543a8fb46b85b7a0d26c5227
    8813da6563a58635e06926530885c53c2df9ba4223c7faec148e5e3f227ace46
    655e7025406f08ae98eea2b1d1aa80213b8370281c5474d386795bd78ef4f204
    aa8a736b1662a3f65cf4b47c3f203d698a47a82aea11ce04a6e223358f63c960
    ea4241f7a5c8631689654653912c7654473962d688469c97381526315203e0a0
    5d4c3e0ec3899a107f75a53ecb7654ac318c93dae4af082e79bcebcbd59b859c
    e9e31490f65b150ca1e8d39498a432f3e6954b0b6e41b150ddc532a86ddb5300
    5431905d05ea6324a976d0ba0846360b2e8e16811cbb7ebd19e08aa12e4c1480
    5a36853ea72db2e419681036feb1f6d76d35b69a236bfd0b069e561f26fd57e5
    b9eee1b6d44dac1eace4d20ed82c6c269663e544e61f119c8087aaf50ab9b546
    68274c64a1ebe1abc2273ce56e199dc615b3787f28e39e59a9a9fe9409da0620
    90dda41805628f6d73a9ff4dba77ca2ca9ee038041bd673274e93963b1cb87e7
    0ab593c899b1f14d862f7d95c1fc8bd91f60eef4c355fb070d45c77fe3051258
    572aab151f64be37ebf2605118b56a657281373b91faf14bd1a5ac7632e07a10
    74'
  }
```

Figure 7: Example FN-DSA-1024 Public COSE Key

A.2.2. COSE Sign1

```
18([
  <<{
    / alg FN-DSA-512 / 1: -54,
  }>>,
  / unprotected / {},
  / payload / h'66616b65',
  / signature /
h'39d79a9d52f6abf0dbfcdd2ae28f612741d41637793a3d698542d69d277ba3cf
  15cb855a7000913b9badc27925ba438ec42d6ff6cd25193528d1c4647555c6be
  6ffd385768dc1b8f1c0ff3989da64c79903f4c6c1fb68922843a7eae3b4d2b16
  cfa8301b07c6556df42ecc5a7d32e6bbfad7f7c144630f377d86429867eeb1d7
  ffa598e78b443a0fc383bfc962e8f22e92e539432d3ee9e396855ea5396e6aaa
  3c1fa95e54fa73f57dd6874ca24f555c7b539172546552fde533dd07033273d5
  f2ccae76ec03a7009e58e735667a58e4a7768732e763dce210d62377f2894bd0
  1778872dce0f68ae2ce4e529ded268707cd552a3a131c944a7756fc2695a4451
  834a673b4df69a1eb9bb2ef4fd29541a7ff206605cd9fa9a4112cba64a01e4be
  6c4f2752d9975ab064b8d7eea8a5f8c407a25ca6ea70f2ef4cbda113ad2bdf1a
  e5e0b2556cc513c5d7e47ef0a79f9df3d6b7ea2ec69f192211b918c1d414e772
  364ca57713459e23d0f8bca12d2213185ece7d58cb0aee9a32f56c28d5759192
  c8ec3147be61aa122f8ca4ad710dfe72caef608cfb8ea4ce7c0cb6e8af22eddc
  cd896fa553ec1184632107d276dc896267ad80d5151d0e6204470c0233a733cc
  b7d3564413cfc26dc48d216871c09118f6d9b1c49f363e32c1347c647e851188
  4a58f6cda5797191da36245f5418b6110f69d061c920840cf3ad67010c6593c5
  5ba37d8b4b72e91a72e6a872379db25e3f07bbba4c91765b1f1f498b2e61f64c
  4da4b2486cf878c76a39b5c7ff53ca036c5ae269e73f37854695067f9d85aa78
  b6e5262a25501d2c8b43923f84195bade108044a270e55ed379ae3193ed115ba
  76cbec7af6314e71a64c3bceae54d7c0135e8c27ae47a61badb9979c73b10647
  3919308cb58efcf27b1537896e86cf182c42'
])
```

Figure 8: Example FN-DSA-512 COSE Sign1

```
18([
  <<{
    / alg FN-DSA-1024 / 1: -55,
  }>>,
  / unprotected / {},
  / payload / h'66616b65',
  / signature /
h'3a12ef94a269b3d76e22c8bb373e940fa78db86f3a5b79544a415eab87f6bea0
  7535d1a75c0c3f1913399592ee4495013006cf21eaf42858bde3dc87d4c9d0df
  3a684a37f876f42e1b5a8208f46da8cddddf737f7a6c5d50fad220da712d62d7
  f3a2671c850366c2756133054a9f54d7109533fba24edbed433cddca8d7226ef
  ec103d5c09153ddba53e4f4afbc330b5f1614f683c8da9c543675fdd6329aca8
  f9e489a69b96df99b886f702485bef87e36a41094682702083aa81c01498b09a
  a3b3fb0f9122bed7f8d55640bbe95e6bd2a0a46274582d2b189ae5c95dc31b40
  31399da49a510f7d5adb451d7162caff632a5e6d8a6b24c465d4794e6e3a9641
  b3647720fa6f4d8f8f9d56c424edabff28d1e81e640930452b111244c6a0f0c9
```

```
    c1b4acee90ed854f7d8acb50ea1f1c9379ca8abb9db6a5b4c9ed685c6689db5a
    72a919ca6f504e37a5f98da26db24b229d6ee4e94b24519c47c25090eddc6363
    adb11bc3154c627a9191af9ba5ca3e9494c0d12ef74ac3306a0b9419aac0f575
    19d60716567f52ce93fdf08eb4db8e5c2d0a6e37b47aac654db5317c97a22134
    3e5ffeb26596c141b60b6ac3706a4ef4b7e27b3666e3ed13c932389170a36ede
    fe0dca4ee4ea26b99ddb363499469daa44d192dd3f796dc8720c86d60c864506
    efc9f59f46ddff7c3f4f0ea75ad4c062bfc89b7021470a3e8baaa8ea2bf1aad4
    539565b04ba878b45b67b280c26e5939c6497570b31df3470386f84f5164d717
    ef7d37659952e2d0129356cefc7118e9ec72846aff9b0502e72d8d6190c4cf2d
    da71f5a79dd396a55f34dab0bd9e28af9960c7197cb2c175fe10114cb2218936
    d7eca6b808efc22f8943f1126d7b4f138f4c1408d6ff5865731936da452b3549
    335ac02e5abaef2ec9a345d8dd8722e9006cd980c4473a6854237cc49b5d3b55
    e998c258ca34edf1e72d4b8c1130e3e6eb1ad6ee2ac9aafc838125622d8be28c
    9288269de3c0c0a04ec4fab8cdba096b83018fecd5e313faf149b7bd8e8495d0
    807388bb6b4d5192e2cb84c2987851cd208189d84f152550e3d9b104205a236c
    92a30d901796df2c63c86620d82bd88302815d2c15e6b222d7fa678ebf65e1de
    e7522e8eb4bfa584ebd9a8e7269377e34a9db2653773835c3a867507d8ac30ec
    d366c356b3af43569244bb73ad2b81c9337e5877648e49daa1a8dc38506b76b7
    6dfbb1f1e225b53a6eb1249137a0e17e72efbe40d34a8a0aaad7c0d986b6e7ab
    89537c56c60d444b61add8cff00b371d60ada9ef3b0df5cb3353470578f8c9c9
    f3dff8cbcb5306be6f7b6a66290ffa54d3958e2c71eefa767f83f35d21104e36
    911767db8e454d37f551f12ecc148b3fe5d8ba95ad0eae06a719961d4822d536
    994699d2999c7982a4113447619f67ea52e48f7a89780852042c73ce356d43c9
    11698c7f419d5b4ae384bcf2e3bb2b846b37906523950a5e315d7b3989162ed6
    5299859ce24a51bcef8724d62852d3ded76e7cc89ac9865393ce7ef33ce85a2a
    0df19e7ad04e7eab47dcb7609e06aaa6c5702630a3af4cb054d17dbbfb582e3f
    825573b44bb7053641dad24ecca10afdfd8d29f5c7484a3f210a54d96fceb0b0
    ffe7dd89fabe4c52e688e1d65425eac9497bb9b213ccd3efd29225a026760629
    1b755a44e64b4690e28b840e1280a49b1b6e4b46bad677c99a62c91de45c7ed0
    68897ee8c3071b9913e0a5653e0a5f165204c8082a97141ab64d41a7b9ccc76c
    9dc82c1044f968b84573c74f7db38da76a349d08579339a1ae40'
  ])
```

Figure 9: Example FN-DSA-1024 COSE Sign1

Acknowledgments

We would like to especially thank David Balenson for careful review of approaches taken in this document. We would also like to thank Michael B. Jones for guidance in authoring.

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