

COSE
Internet-Draft
Intended status: Standards Track
Expires: 7 May 2026

E. Lundberg, Ed.
Yubico
M. B. Jones
Self-Issued Consulting
3 November 2025

Split signing algorithms for COSE
draft-lundberg-cose-two-party-signing-algs-03

Abstract

This specification defines COSE algorithm identifiers for negotiating how to split a signature algorithm between two cooperating parties. Typically the first party hashes the data to be signed and the second party finishes the signature over the hashed data. This is a common technique, useful for example when the signing private key is held in a smart card or similar hardware component with limited processing power and communication bandwidth. The resulting signatures are identical in structure to those computed by a single party, and can be verified using the same verification algorithm without additional steps to preprocess the signed data.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at
<https://datatracker.ietf.org/doc/draft-lundberg-cose-two-party-signing-algs/>.

Discussion of this document takes place on the COSE 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/YubicoLabs/cose-two-party-signing-algs-rfc>.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 7 May 2026.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	3
1.1. Requirements Notation and Conventions	4
2. Split Signing Algorithms	4
2.1. ECDSA	5
2.2. HashEdDSA	5
3. COSE Signing Arguments	7
3.1. COSE Signing Arguments Common Parameters	8
4. Security Considerations	9
4.1. Protocol-Level Trusted Roles	9
4.2. Component-Level Trusted Roles	9
5. IANA Considerations	10
5.1. COSE Algorithms Registrations	10
5.2. COSE Signing Arguments Common Parameters Registry	12
5.3. COSE Signing Arguments Algorithm Parameters Registry	12
6. References	12
6.1. Normative References	12
6.2. Informative References	13
Document History	14
Authors' Addresses	15

1. Introduction

CBOR Object Signing and Encryption (COSE) [RFC9052] algorithm identifiers are used for algorithm negotiation and to annotate cryptographic objects with how to interpret them, for example which algorithm to use to verify a signature or decapsulate a shared key. Existing COSE algorithm identifiers omit some internal details of how the object was constructed, since those details are typically irrelevant for the recipient.

The algorithm identifiers defined in this specification are meant for a complementary use case: to divide responsibilities during construction of a cryptographic object, instead of describing how to consume the object. Specifically, they provide an interoperable way to negotiate how a signing operation is split between two cooperating parties, for example, a smart card and a software application, while the verification algorithm for the resulting signature remains the same as if the signature was created by a single party. These split algorithm identifiers are therefore not meant for annotating signature objects, since the verification algorithm is better indicated using already existing algorithm identifiers.

As mentioned above, a primary use case for this is for algorithm negotiation between a software application and a smart card or other hardware security module (HSM) holding the signing private key. Since the HSM may have limited processing power and communication bandwidth, it may not be practical to send the entire original message to the HSM. Instead, since most signature algorithms begin with digesting the message into a fixed-length intermediate input, this initial digest can be computed by the software application while the HSM performs the rest of the signature algorithm on the digest. This is a common technique used in standards such as OpenPGP [OPENPGPCARD], PKCS #11 [PKCS11-Spec-v3.1], and PIV [FIPS-201].

Since different signature algorithms digest the message in different ways and at different stages of the algorithm, it is not possible for a cryptographic API to specify that, for example, "the hash digest is computed by the caller" generically for all algorithms. Instead, the algorithm identifiers defined in this specification enable the parties of that cryptographic API to signal precisely, for each signature algorithm individually, which steps of the algorithm are performed by which party. We thus define two roles: the digester (e.g., a software application) that initializes the signing procedure, and the signer (e.g., an HSM) that holds exclusive control of the signing private key.

Note that these algorithm identifiers do not define new "pre-hashed" variants of the base signature algorithm, nor an intermediate "hash envelope" data structure, such as that defined in [I-D.COSE-Hash-Envelope]. Rather, these identifiers denote existing signature algorithms that would typically be executed by a single party, but split into two stages.

Some signature algorithms, such as PureEdDSA [RFC8032], by their design, cannot be split in this way, and therefore cannot be assigned split signing algorithm identifiers. However, if such a signature algorithm defines a "pre-hashed" variant, such as Ed25519ph [RFC8032], that "pre-hashed" algorithm can be assigned a split signing algorithm identifier, enabling the pre-hashing step to be performed by the `_digerster_` and the remaining steps by the `_signer_`.

1.1. Requirements Notation and Conventions

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.

2. Split Signing Algorithms

This section defines divisions of signing algorithm steps between a `_digerster_` and a `_signer_` in a split signing protocol, and assigns algorithm identifiers to these algorithm divisions. The `_digerster_` performs the first part of the split algorithm and does not have access to the signing private key, while the `_signer_` performs the second part of the split algorithm and has access to the signing private key. For signing algorithms that format the message to insert domain separation tags, as described in Section 2.2.5 of [RFC9380], this message formatting is also performed by the `_signer_`.

The algorithm identifiers defined in this specification MAY appear in COSE structures used internally between the `_digerster_` and the `_signer_` in a split signing protocol, but SHOULD NOT appear in COSE structures consumed by signature verifiers. COSE structures consumed by signature verifiers SHOULD instead use the corresponding conventional algorithm identifiers for the verification algorithm. These are listed in the "Verification algorithm" column in the tables defining split signing algorithm identifiers.

2.1. ECDSA

ECDSA [FIPS-186-5] split signing uses the following division between the `_digerster_` and the `_signer_` of the steps of the ECDSA signature generation algorithm [FIPS-186-5]:

- * The signing procedure is defined in Section 6.4.1 of [FIPS-186-5].
- * The `_digerster_` performs Step 1 of the signing procedure - hashing the message, producing the value `_H_`.
- * The message input to the `_signer_` is the value `_H_` defined in the signing procedure.
- * The `_signer_` resumes the signing procedure from Step 2.

The following algorithm identifiers are defined:

Name	COSE Value	Verification algorithm	Description
ESP256-split	TBD	ESP256	ESP256 split signing as defined in Section 2.1
ESP384-split	TBD	ESP384	ESP384 split signing as defined in Section 2.1
ESP512-split	TBD	ESP512	ESP512 split signing as defined in Section 2.1

Table 1: ECDSA split signing algorithm values.

Note: This is distinct from the similarly named Split-ECDSA (SECDSA) [SECDSA], although SECDSA can be implemented using this split procedure as a component.

2.2. HashEdDSA

Split HashEdDSA [RFC8032] uses the following division between the `_digerster_` and the `_signer_` of the steps of the HashEdDSA signing algorithm [RFC8032]:

- * HashEdDSA is a combination of the EdDSA signing procedure and the PureEdDSA signing procedure. The EdDSA signing procedure is defined in the first paragraph of Section 3.3 of [RFC8032]. The PureEdDSA signing procedure is defined in the second paragraph of Section 3.3 of [RFC8032].
- * The `_digerster_` computes the value $PH(M)$ defined in the EdDSA signing procedure.
- * The message input to the `_signer_` is the value $PH(M)$ defined in the EdDSA signing procedure. This value is represented as M in the PureEdDSA signing procedure.
- * The `_signer_` executes the PureEdDSA signing procedure, where the value denoted M in the PureEdDSA signing procedure takes the value denoted $PH(M)$ in the EdDSA signing procedure.

PureEdDSA [RFC8032] cannot be divided in this way since such a division would require that the `_digerster_` has access to the private key.

The following algorithm identifiers are defined:

Name	COSE Value	Verification algorithm	Description
Ed25519ph	TBD	Ed25519ph	EdDSA using the Ed25519ph parameter set in Section 5.1 of [RFC8032]
Ed25519ph-split	TBD	Ed25519ph	EdDSA using the Ed25519ph parameter set in Section 5.1 of [RFC8032] and split as defined in Section 2.2
Ed448ph	TBD	Ed448ph	EdDSA using the Ed448ph parameter set in Section 5.2 of [RFC8032]
Ed448ph-split	TBD	Ed448ph	EdDSA using the Ed448ph parameter set in Section 5.2 of [RFC8032] and split as defined in Section 2.2

Table 2: HashEdDSA algorithm values.

3. COSE Signing Arguments

While many signature algorithms take the private key and data to be signed as the only two parameters, some signature algorithms have additional parameters that must also be set. For example, to sign using a key derived by ARKG [I-D.bradleylundberg-ARKG], two additional arguments `kh` and `ctx` are needed in ARKG-Derive-Private-Key to derive the signing private key.

While such additional arguments are simple to provide to the API of the signing procedure in a single-party context, in a split signing context these additional arguments also need to be conveyed from the `_digester_` to the `_signer_`. For this purpose, we define a new COSE structure `COSE_Sign_Args` for "COSE signing arguments". This enables defining a unified, algorithm-agnostic protocol between the `_digester_` and the `_signer_`, rather than requiring a distinct protocol for each signature algorithm for the sake of conveying algorithm-specific parameters.

COSE_Sign_Args is built on a CBOR map. The set of common parameters that can appear in a COSE_Sign_Args can be found in the IANA "COSE Signing Arguments Common Parameters" registry (TODO). Additional parameters defined for specific signing algorithms can be found in the IANA "COSE Signing Arguments Algorithm Parameters" registry (TODO).

The CDDL grammar describing COSE_Sign_Args, using the CDDL fragment defined in Section 1.5 of [RFC9052], is:

```
COSE_Sign_Args = {
    3 ^ => tstr / int,  ; alg
    * label => values,
}
```

3.1. COSE Signing Arguments Common Parameters

This document defines a set of common parameters for a COSE Signing Arguments object. Table 3 provides a summary of the parameters defined in this section.

Name	Label	CBOR Type	Value Registry	Description
alg	3	tstr / int	COSE Algorithms	Signing algorithm to use

Table 3: Common parameters of the COSE_Sign_Args structure.

- * alg: This parameter identifies the signing algorithm the additional arguments apply to. The signer MUST verify that this algorithm matches any key usage restrictions set on the key to be used. If the algorithms do not match, then the signature operation MUST be aborted with an error.

Definitions of COSE algorithms MAY define additional algorithm-specific parameters for COSE_Sign_Args.

The following CDDL example conveys additional arguments for signing data using the ESP256-split algorithm (see Section 2.1) and a key derived using ARKG-P256 [I-D.bradleylundberg-ARKG]:


```
{
  3: -65539,      ; alg: ESP256-split with ARKG-P256 (placeholder value)

                  ; ARKG-P256 key handle
                  ; (HMAC-SHA-256-128 followed by
                  ;   SEC1 uncompressed ECDH public key)
  -1: h'27987995f184a44cfa548d104b0a461d
      0487fc739dbcdabc293ac5469221da91b220e04c681074ec4692a76ffacb9043de
      c2847ea9060fd42da267f66852e63589f0c00dc88f290d660c65a65a50c86361',

                  ; ctx argument to ARKG-Derive-Private-Key
  -2: 'ARKG-P256.test vectors',
}
```

4. Security Considerations

4.1. Protocol-Level Trusted Roles

This specification assumes that both the `_digerster_` and `_signer_` roles described in Section 2 are trusted and cooperate honestly. This is because these split signing procedures concern details that are considered implementation details from a verifier's perspective. When a signature is generated by a single party, that single party takes on both the `_digerster_` and the `_signer_` roles, and obviously trusts itself to perform the `_digerster_` role honestly. This assumption is carried forward for the split signing use case: the `_digerster_` is assumed trusted, since it is part of the overall procedure of generating a signature over some input data. From the verifier's perspective, a malicious `_digerster_` in the split signing model would have the same powers as a malicious signature generator in a single-party signing model. Thus, on the application or protocol level, assuming an honest `_digerster_` is no more restrictive than assuming an honest signature generator.

4.2. Component-Level Trusted Roles

The reasoning in Section 4.1 does not hold on the component level. A `_signer_` implementation MUST NOT assume that the `_digerster_` implementation it interoperates with is necessarily honest. Split signing algorithms MUST NOT be defined in a way that enables a malicious `_digerster_` with access to an honest `_signer_` to produce forgeries or extract secrets from the `_signer_`.

For example, for ECDSA (Section 2.1), a malicious `_digerster_` can choose `_H_` in such a way that the `_signer_` will derive any `_digerster_-`chosen value of `_e_`, including zero or other potentially problematic values. Fortunately, in this case, this does not enable the `_digerster_` to extract the signature nonce or private key. It

also does not enable forgeries, since the `_digester_` still needs to find a preimage of `_e_` for the relevant hash function. Definitions of other algorithms need to ensure that similar chosen-input attacks do not enable extracting secrets or forging protocol-level messages.

5. IANA Considerations

5.1. COSE Algorithms Registrations

This section registers the following values in the IANA "COSE Algorithms" registry [IANA.COSE]:

- * Name: ESP256-split
 - Value: TBD (Requested Assignment -300)
 - Description: ESP256 split signing
 - Capabilities: [kty]
 - Change Controller: IETF
 - Reference: Section 2.1 of this specification
 - Recommended: Yes
- * Name: ESP384-split
 - Value: TBD (Requested Assignment -301)
 - Description: ESP384 split signing
 - Capabilities: [kty]
 - Change Controller: IETF
 - Reference: Section 2.1 of this specification
 - Recommended: Yes
- * Name: ESP512-split
 - Value: TBD (Requested Assignment -302)
 - Description: ESP512 split signing
 - Capabilities: [kty]

- Change Controller: IETF
 - Reference: Section 2.1 of this specification
 - Recommended: Yes
- * Name: Ed25519ph
- Value: TBD
 - Description: EdDSA using the Ed25519ph parameter set in Section 5.1 of [RFC8032]
 - Capabilities: [kty]
 - Change Controller: IETF
 - Reference: Section 5.1 of [RFC8032]
 - Recommended: Yes
- * Name: Ed25519ph-split
- Value: TBD (Requested Assignment -303)
 - Description: Ed25519ph split as defined in Section 2.2
 - Capabilities: [kty]
 - Change Controller: IETF
 - Reference: Section 2.2 of this specification
 - Recommended: Yes
- * Name: Ed448ph
- Value: TBD
 - Description: EdDSA using the Ed448ph parameter set in Section 5.2 of [RFC8032]
 - Capabilities: [kty]
 - Change Controller: IETF
 - Reference: Section 5.2 of [RFC8032]

- Recommended: Yes

* Name: Ed448ph-split

- Value: TBD (Requested Assignment -304)
- Description: Ed448ph split as defined in Section 2.2
- Capabilities: [kty]
- Change Controller: IETF
- Reference: Section 2.2 of this specification
- Recommended: Yes

5.2. COSE Signing Arguments Common Parameters Registry

TODO

5.3. COSE Signing Arguments Algorithm Parameters Registry

TODO

6. References

6.1. Normative References

[I-D.bradleylundberg-ARKG]

Lundberg, E. and J. Bradley, "The Asynchronous Remote Key Generation (ARKG) algorithm", Work in Progress, Internet-Draft, draft-bradleylundberg-cfrg-arkg-09, 7 July 2025, <<https://datatracker.ietf.org/doc/html/draft-bradleylundberg-cfrg-arkg-09>>.

[IANA.COSE]

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

[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>>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <<https://www.rfc-editor.org/rfc/rfc8032>>.

- [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>>.
- [RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <<https://www.rfc-editor.org/rfc/rfc8610>>.
- [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>>.
- [RFC9864] Jones, M.B. and O. Steele, "Fully-Specified Algorithms for JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE)", RFC 9864, DOI 10.17487/RFC9864, October 2025, <<https://www.rfc-editor.org/rfc/rfc9864>>.
- [SEC1] Certicom Research, "SEC 1: Elliptic Curve Cryptography", May 2009, <<https://www.secg.org/sec1-v2.pdf>>.

6.2. Informative References

- [FIPS-186-5] National Institute of Standards and Technology, "Digital Signature Standard (DSS)", February 2023, <<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf>>.
- [FIPS-201] Ferraiolo, H., Mehta, K., Francomacaro, S., Chandramouli, R., and S. Gupta, "Interfaces for Personal Identity Verification: Part 2 PIV Card Application Card Command Interface", NIST Special Publication (SP) NIST SP 800-73pt2-5, 2024, <<https://doi.org/10.6028/NIST.SP.800-73pt2-5>>.
- [FIPS-204] National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard", August 2024, <<https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf>>.

[I-D.COSE-Hash-Envelope]

Steele, O., Lasker, S., and H. Birkholz, "COSE Hash Envelope", Work in Progress, Internet-Draft, draft-ietf-cose-hash-envelope-09, 22 October 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-cose-hash-envelope-09>>.

[OPENPGPCARD]

Pietig, A., "Functional Specification of the OpenPGP application on ISO Smart Card Operating Systems", Version 3.4.1, March 2020, <<https://gnupg.org/ftp/specs/OpenPGP-smart-card-application-3.4.1.pdf>>.

[PKCS11-Spec-v3.1]

Bong, D. and T. Cox, "PKCS #11 Specification Version 3.1.", OASIS Standard, 23 July 2023, <<https://docs.oasis-open.org/pkcs11/pkcs11-spec/v3.1/os/pkcs11-spec-v3.1-os.html>>. Latest stage: <https://docs.oasis-open.org/pkcs11/pkcs11-spec/v3.1/pkcs11-spec-v3.1.html> (<https://docs.oasis-open.org/pkcs11/pkcs11-spec/v3.1/pkcs11-spec-v3.1.html>).

[RFC9380]

Faz-Hernandez, A., Scott, S., Sullivan, N., Wahby, R. S., and C. A. Wood, "Hashing to Elliptic Curves", RFC 9380, DOI 10.17487/RFC9380, August 2023, <<https://www.rfc-editor.org/rfc/rfc9380>>.

[SECDSA]

Verheul, E., "SECDSA: Mobile signing and authentication under classical "sole control"", July 2021, <<https://eprint.iacr.org/2021/910>>.

Document History

-03

- * Updated reference to ARKG parameter info renamed to ctx.
- * Refined abstract and introduction to emphasize that the central novelty is not split algorithms as a concept, but providing COSE algorithm identifiers for use cases that benefit from such splitting.
- * Replaced reference to draft-ietf-jose-fully-specified-algorithms with RFC 9864.

- * Added inline definitions of Ed25519ph and Ed448ph registrations, replacing speculative references to registrations that do not exist elsewhere.
- * Added missing captions to Tables 1 and 2.
- * Added Security Considerations section.

-02

- * Renamed document from "COSE Algorithms for Two-Party Signing" to "Split signing algorithms for COSE" and updated introduction and terminology accordingly.
- * Dropped definitions for HashML-DSA, as split variants of ML-DSA are being actively discussed in other IETF groups.
- * Changed "Base algorithm" heading in definition tables to "Verification algorithm".
- * Remodeled COSE_Key_Ref as COSE_Sign_Args.
 - Dropped definitions of reference types for COSE Key Types registry.

-01

- * Added IANA registration requests for algorithms defined.
- * Updated references and other editorial tweaks.

-00

- * Initial individual draft

Authors' Addresses

Emil Lundberg (editor)
Yubico
Gvlegatan 22
Stockholm
Sweden
Email: emil@emlun.se

Michael B. Jones
Self-Issued Consulting
United States

Email: michael_b_jones@hotmail.com

URI: <https://self-issued.info/>