COSE Working Group
Internet-Draft
Intended status: Informational
Expires: 13 March 2026

D. Ochkas
H. Le Bouder
A. Pelov
IMT Atlantique

9 September 2025

Ascon-AEAD128 for COSE and JOSE
draft-ochkas-cose-ascon-02

Abstract

This document describes CBOR Object Signing and Encryption (COSE) and JSON Object Signing and Encryption (JOSE) serializations with Ascon which is a NIST standard for lightweight cryptography.

In 2019, as a part of CAESAR competition, Ascon-128 and Ascon-128a were selected as the first choice for the lightweight authenticated encryption [asconv1.2-caesar]. After, in 2023, National Institute of Standards and Technology (NIST) selected Ascon family of cryptographic algorithms to be the standard for lightweight cryptography [asconv1.2-nist]. In August 2025, NIST Special Publication 800-232 was released, defining Ascon-based lightweight cryptography standards for constrained devices [NIST.SP.800-232]. This recognition makes it particularly interesting to use Ascon with COSE and JOSE structures.

This document does not define any new cryptography, only serializations of existing cryptographic systems described in [NIST.SP.800-232].

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 13 March 2026.

Table of Contents

1. Introduction

Constrained networks such as Internet of Things (IoT) networks most of the time are characterized by the limited computational power and autonomy. In this context, the choice of suitable cryptographic algorithms that provide robust security without consuming large amount of resources is essential. As a winner of the lightweight cryptography standardization process conducted by NIST, Ascon family of cryptographic algorithms is a perfect candidate for the described

situation.

Ascon-Based Lightweight Cryptography Standards for Constrained Devices [NIST.SP.800-232] introduces a suite of algorithms consisting of Authenticated Encryption with Associated Data (AEAD), a hash function, and two eXtendable Output Functions (XOFs).

This document focuses on the AEAD part of Ascon standard. It enables the usage of Ascon-AEAD128 with COSE and JOSE for content encryption.

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. Ascon algorithms

In the scope of this document, only the authenticated encryption scheme of the Ascon family is allowed for, namely Ascon-AEAD128. Ascon-AEAD128.enc and Ascon-AEAD128.dec algorithms are parametrized by the key size k, the nonce size n, the tag size t, the rate r, and the internal round numbers a and b. [NIST.SP.800-232] specifies the Ascon-AEAD128 algorithm with the following parameters:

Key size, k	Nonce size, n	Tag size, t	Rate, r	Outer permutation rounds, a	Inner permutation rounds, b
128 bits	128 bits	128 bits	128 bits	12	8

Table 1: Ascon-AEAD128 parameters

In addition, [NIST.SP.800-232] allows the tag truncation. The standard permits tag sizes 了, where 32 <= 了 <= 128 bits. Tags of less than 64 bits SHALL only be selected after a careful risk analysis.

Since COSE can be used in different scenarios, this document requests to register three variations of Ascon-AEAD128 in [IANA.cose] with common tag sizes of 32, 64, and 128 bits (see Table 2). Using the 32-bit variation is discouraged for typical scenarios and SHOULD be introduced only in extremely constrained use cases with justified security.

Name	alg	Description
Ascon-AEAD128	TBD (requested assignment 35)	Ascon-AEAD128 with 128-bit tag as the CBOR Object Encryption Algorithm
Ascon-AEAD128/64	TBD (requested assignment 36)	Ascon-AEAD128 with 64-bit tag as the CBOR Object Encryption Algorithm
Ascon-AEAD128/32	TBD (requested assignment 37)	Ascon-AEAD128 with 32-bit tag as the CBOR Object Encryption Algorithm

Table 2: COSE Algorithms for Ascon

In COSE, keys may be obtained from either a key structure or a recipient structure [RFC9052].

When using a COSE key for this algorithm, the following checks are made:

* The "kty" field MUST be present, and it MUST be "Symmetric".

* If the "alg" field is present, it MUST match the variation of Ascon-AEAD128 algorithm being used.

* If the "key_ops" field is present, it MUST include "encrypt" when encrypting.

* If the "key_ops" field is present, it MUST include "decrypt" when decrypting.

COSE encryption and decryption with Ascon-AEAD128 is done in accordance with Section 5.3 of [RFC9052].

Also, this document requests the registration of the Ascon-AEAD128 algorithms in [IANA.jose] with 64-, and 128-bit tags (see Table 3). Unlike COSE, there is no 32-bit tag variation since JSON Web Encryption (JWE) structure is not intended to be used in extremely constrained scenarios.

Name	enc	Description
Ascon-AEAD128	Ascon-AEAD128	Ascon-AEAD128 with 128-bit tag as the JSON Object Encryption Algorithm
Ascon-AEAD128/64	Ascon-AEAD128/64	Ascon-AEAD128 with 64-bit tag as the JSON Object Encryption Algorithm

Table 3: JOSE Algorithms for Ascon

JOSE encryption and decryption processes with Ascon-AEAD128 should follow Section 5 of [RFC7516].

Implementations that are encrypting or decrypting MUST validate that the key type, key length, and algorithm are correct and appropriate for the entities involved.

4. IV Header Parameter

Unlike some common AEAD algorithms, Ascon distinguishes between the notion of initialization vector (IV) and nonce (N). While N is the input argument for the Ascon-AEAD128 encryption/decryption functions, IV is the constant defined for each Ascon algorithm used as a part of state initialization.

However, [IANA.cose] does not define a separate header parameter to specify Nonce. Thus, in COSE, whenever Full Initialization Vector Header Parameter (Name: IV, Label: 5) or Partial Initialization Vector Header Parameter (Name: Partial IV, Label: 6) is specified it SHALL refer to the N argument of the corresponding Ascon function.

On the other hand, JSON Web Signature and Encryption Header Parameters registry at [IANA.jose] defines both Nonce Header Parameter ("nonce") and Initialization Vector Header Parameter ("iv"). However, the "nonce" parameter is intended to be used only with signatures. Therefore, in JOSE, "iv" parameters SHALL refer to the N argument of the corresponding Ascon function. There SHOULD NOT be "nonce" parameters specified while using Ascon for content encryption. In case "nonce" parameter is specified it MUST be ignored.

5. Security Considerations

The security considerations for [NIST.SP.800-232], [RFC7516], [RFC7517] and [RFC9052] apply to this specification as well.

According to the most recent security analysis publications, Ascon did not show any security vulnerabilities so far and the best attacks target the initialization of Ascon reduced to 7 (out of 12) rounds, concluding that Ascon has a security margin of 5 rounds (42 % of the 12 rounds). More details are available at List of Published Analysis section of [asconv1.2-nist].

6. IANA Considerations

6.1. Additions to Existing Registries

6.1.1. 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]. The "Recommended" field for Ascon-AEAD128/32 is set to "Filter Only" to discourage unreflected usage.

6.1.1.1. Ascon-AEAD128 for COSE

* Name: Ascon-AEAD128
* Value: TBD (requested assignment 35)
* Description: Ascon-AEAD128 with 128-bit tag
* Capabilities: [kty]
* Reference: NIST SP 800-232
* Recommended: Yes

6.1.1.2. Ascon-AEAD128/64 for COSE

* Name: Ascon-AEAD128/64
* Value: TBD (requested assignment 36)
* Description: Ascon-AEAD128 with 64-bit tag
* Capabilities: [kty]
* Reference: NIST SP 800-232
* Recommended: Yes

6.1.1.3. Ascon-AEAD128/32 for COSE

* Name: Ascon-AEAD128/32
* Value: TBD (requested assignment 37)
* Description: Ascon-AEAD128 with 32-bit tag
* Capabilities: [kty]
* Reference: NIST SP 800-232
* Recommended: Filter Only

6.1.2. 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].

6.1.2.1. Ascon-AEAD128 for JOSE

* Algorithm Name: Ascon-AEAD128
* Algorithm Description: Ascon-AEAD128 with 128-bit tag
* Algorithm Usage Location(s): enc
* JOSE Implementation Requirements: Optional
* Change Controller: IESG
* Specification Document(s): NIST SP 800-232

* Algorithm Analysis Documents(s): n/a

6.1.2.2. Ascon-AEAD128/64 for JOSE

* Algorithm Name: Ascon-AEAD128/64
* Algorithm Description: Ascon-AEAD128 with 64-bit tag
* Algorithm Usage Location(s): enc
* JOSE Implementation Requirements: Optional
* Change Controller: IESG
* Specification Document(s): NIST SP 800-232
* Algorithm Analysis Documents(s): n/a

7. References

7.1. Normative References

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

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

[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>.

[RFC7516] Jones, M. and J. Hildebrand, "JSON Web Encryption (JWE)", RFC 7516, DOI 10.17487/RFC7516, May 2015, <https://www.rfc-editor.org/rfc/rfc7516>.

[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>.

7.2. Informative References

[asconv1.2-caesar]
Dobraunig, C., Eichlseder, M., Mendel, F., and M. Schl辰ffer, "Ascon v1.2, Submission to Round 3 of the CAESAR competition", 2016, <https://competitions.cr.yp.to/round3/asconv12.pdf>.

[asconv1.2-nist]
Dobraunig, C., Eichlseder, M., Mendel, F., and M. Schl辰ffer, "Ascon v1.2, Submission to Final Round of the NIST Lightweight Cryptography project", 2021, <https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/ascon-spec-final.pdf>.

[NIST.SP.800-232]
Turan, M. S., McKay, K. A., Kang, J., and J. Kelsey, "Ascon-Based Lightweight Cryptography Standards for Constrained Devices", DOI 10.6028/NIST.SP.800-232, August 2025, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-232.pdf>.

Appendix A. Examples

This appendix provides some examples of various Ascon-AEAD128 Encryptions with COSE and JOSE

A.1. COSE

A.1.1. Simple Ascon-AEAD128 encryption

```
{
  "plaintext": "This is the content.",
  "nonce_hex": "00000000000000000000000000000000",
  "AAD_hex": "8367456E637279707443A1010140",
  "CEK_hex": "849B57219DAE48DE646D07DBB533566E",
  "Encrypt0_hex": "8344A1011823A10550000000000000000000000000000000582461484F95FC36BD13
D7EFCA1C370EE3B6A1125770C8878467D3AE466C7C6CC4F4918BAA96",
  "Encrypt0_diag": "[h'A1011823', {5: h'00000000000000000000000000000000'}, h'61484F95FC3
6BD13D7EFCA1C370EE3B6A1125770C8878467D3AE466C7C6CC4F4918BAA96']"
}
```


A.1.2. Direct Ascon-AEAD128 encryption with recipient


```
{
  "plaintext": "This is the content.",
  "nonce_hex": "00000000000000000000000000000000",
  "AAD_hex": "8367456E637279707443A1010140",
  "CEK_hex": "849B57219DAE48DE646D07DBB533566E",
  "key": {
    "kid": "abcdef",
    "kty": "Symmetric"
  },
  "Encrypt": "8444A1011823A10550000000000000000000000000000000005824D3468D9110A2C3005E82D
48628CD462BBD8721FBABE883A7743F191AC81CA8D6BBED5E44818340A2012504466162636465640",
  "Encrypt_diag": "[h'A1011823', {5: h'00000000000000000000000000000000'}, h'D3468D9110A2
C3005E82D48628CD462BBD8721FBABE883A7743F191AC81CA8D6BBED5E44', [[h'', {1: -6, 4: h'616263
646566'}, h'']]]"
}
```


A.1.3. Direct Ascon-AEAD128 encryption with HKDF-SHA-256


```
{
  "plaintext": "This is the content.",
  "nonce_hex": "00000000000000000000000000000000",
  "AAD_hex": "8367456E637279707443A1010140",
  "CEK_hex": "849B57219DAE48DE646D07DBB533566E",
  "key": {
    "kid": "abcdef",
    "kty": "Symmetric"
  },
  "salt": "abcdefghijlmnopq",
  "Encrypt": "8444A1011823A10550000000000000000000000000000000005824B80EA16F0EBCC9F25502E
E1D992D23C4E7984E2919AD6C3E37581FB099DB5855F1490ECF818340A3012933506162636465666768696A6C
6D6E6F70710446616263646564 0",
  "Encrypt_diag": "[h'A1011823', {5: h'00000000000000000000000000000000'}, h'B80EA16F0EBC
C9F25502EE1D992D23C4E7984E2919AD6C3E37581FB099DB5855F1490ECF', [[h'', {1: -10, -20: h'616
2636465666768696A6C6D6E6F7071', 4: h'616263646566'}, h'']]]"
}
```


A.2. JOSE

The examples use the following plaintext and cek:


```
{
  "plaintext": "This is the content.",
  "CEK_hex": "849B57219DAE48DE646D07DBB533566E"
}
```

A.2.1. JWE structure with direct Ascon-AEAD128 encryption

```
{
  "protected": "eyJhbGciOiJkaXIiLCJlbmMiOiJBc2Nvbi1BRUFEMTI4In0", \* {"alg": "dir", "enc"
: "Ascon-AEAD128"} *\
  "aad": "g2dFbmNyeXB0Q6EBAUE",
  "encrypted_key": "",
  "iv": "AAAAAAAAAAAAAAAAAAAAAA",
  "tag": "EihrljYH6xrt08Ae9Slqzw",
  "ciphertext": "dMbnoonoAEUph2N4KWIj_i_L-oo"
}
```

A.2.2. JWE structure with Ascon-AEAD128 encryption and AES-128 Key Wrap

```
{
  "protected": "eyJhbGciOiJBMTI4S1ciLCJlbmMiOiJBc2Nvbi1BRUFEMTI4Iiwia2lkIjoiYWJjZGVmIn0",
 \* {"alg":"A128KW","enc":"Ascon-AEAD128","kid":"abcdef"} *\
  "aad": "g2dFbmNyeXB0Q6EBAUE",
  "header": {
    "alg": "A128KW",
    "kid": "abcdef"
  },
  "encrypted_key": "V4d7CMPzWA3ntHiL4gcN5EYoQJX2t-Gw",
  "iv": "AAAAAAAAAAAAAAAAAAAAAA",
  "tag": "9vY9jDG2LZOVmHsD6kHgkA",
  "ciphertext": "wZJfEzhC59fiqtnKtYpXqCi0-Xo"
}
```

Authors' Addresses

Dmytro Ochkas
IMT Atlantique
Email: dmytro.ochkas@imt-atlantique.fr

H辿l竪ne Le Bouder
IMT Atlantique
Email: helene.le-bouder@imt-atlantique.fr

Alexander Pelov
IMT Atlantique
Email: alexander.pelov@imt-atlantique.fr