



**IMT Atlantique**  
Bretagne-Pays de la Loire  
École Mines-Télécom

# Ascon-AEAD128 for JOSE and COSE

draft-ochkas-cose-ascon

D. Ochkas, H. Le Boudier, A. Pelov

IETF 123 Madrid



# Agenda

- Background
- Draft Proposal
- Examples

# Background

- Research on lightweight cryptography for constrained networks
- Investigating end-to-end encryption possibilities in extreme environments (e. g. underwater)
- Use of standardized IoT communication stack: **SCHC/IPv6/UDP/CoAP/OSCORE**
- Need for a lightweight encryption algorithm for **COSE**
- **Ascon** is a NIST selection for lightweight cryptography, see [NIST.SP.800-232](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-232.pdf)

# Draft Proposal

## Ascon-AEAD128 for COSE

- Ascon public draft consists of AEAD, has function and two eXtendable Output Functions (XOFs)
- Draft requests to introduce only Ascon-AEAD128 for COSE
- **Initialization Vector** (Name: IV, Label: 5) or **Partial Initialization Vector** (Name: Partial IV, Label: 6) header parameters should be used to define nonce
- Keys may be obtained from either a **COSE\_Key** or a **COSE\_recipient** structure

# Draft Proposal

## COSE\_Key with Ascon-AEAD128

- The "kty" field MUST be present, and it MUST be "Symmetric".
- If the "alg" field is present, it MUST match the Ascon-AEAD128 (35) 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.

# Draft Proposal

## IANA Modifications

COSE Algorithms new entry:

- \* Name: Ascon-AEAD128
- \* Value: TBD (requested assignment 35)
- \* Description: CBOR Object Encryption Algorithm with Ascon-AEAD128
- \* Capabilities: [kty]
- \* Reference: NIST SP 800-232
- \* Recommended: Yes

# Examples

## Encrypt0 Message

```
[  
  h'A1011823',                /* Protected Headers */  
  {5: 'abcdefghijklmnop'},    /* Public Headers (IV) */  
  h'D3812EB44AD4AFB947A544B99BFDC0AFBB' /* Ascon encrypted content + 16-byte tag */  
]
```

# Examples

## Encrypt Message

```
[
  h'A1011823', /* Protected Headers */
  {5: 'abcdefghijklmnpq'}, /* Public Headers (IV) */
  h'D98EF1006E80EA8E56D1BD9E809B608E60', /* Ascon encrypted content + 16-byte tag */
  [
    [' ', /* Recipient 1 */
     {
       1: -6, /* Direct */
       4: 'abcdef' /* Key ID */
     },
    ' ' ]
  ]
]
```

# Examples

## Encrypt Message with HKDF-SHA-256

```
[
  h'A1011823',                               /* Protected Headers */
  {5: 'abcdefghijklmnpq'},                    /* Public Headers (IV) */
  h'CC23BBAE92C1B49434AD34D9D542BF01BC', /* Ascon encrypted content + 16-byte tag */
  [
    [h'A10129',                               /* Recipient 1 */
     {                                         /* direct+HKDF-SHA-256 */
       -20: 'abcdefghijklmnpq',              /* HKDF Salt */
       4: 'abcdef'                           /* Key ID */
     },
    '' ]
  ]
]
```

# Next Steps

- Foster the interest to Ascon with COSE and JOSE at IETF
- Seek collaboration
- Add full implementations for COSE and JOSE with Ascon in C
- Consult about the draft and address follow up comments