

July 23rd, 2026

Ascon-AEAD128 and Ascon-Hash256 for COSE

Authors: Dmytro Ochkas, H  l  ne Le Boudier, Alexander Pelov

Presenter: Dmytro Ochkas (dmytro.ochkas@imt-atlantique.fr)

IETF 126, Vienna



Proposal

- Ascon family of algorithms is a NIST standard for lightweight cryptography since August 2025.
- COSE is designed for constrained systems, making Ascon a good choice for COSE use cases.
- The standard introduces **Ascon-AEAD128**, **Ascon-Hash256**, and 2 XOFs.

From last year

- COSE encryption with Ascon AEAD.
- 3 modes are introduced:
 - **Ascon-AEAD128** with 128-bit tag.
 - **Ascon-AEAD128-64** with 64-bit tag.
 - **Ascon-AEAD128-32** with 32-bit tag (Filter only).
- Examples.

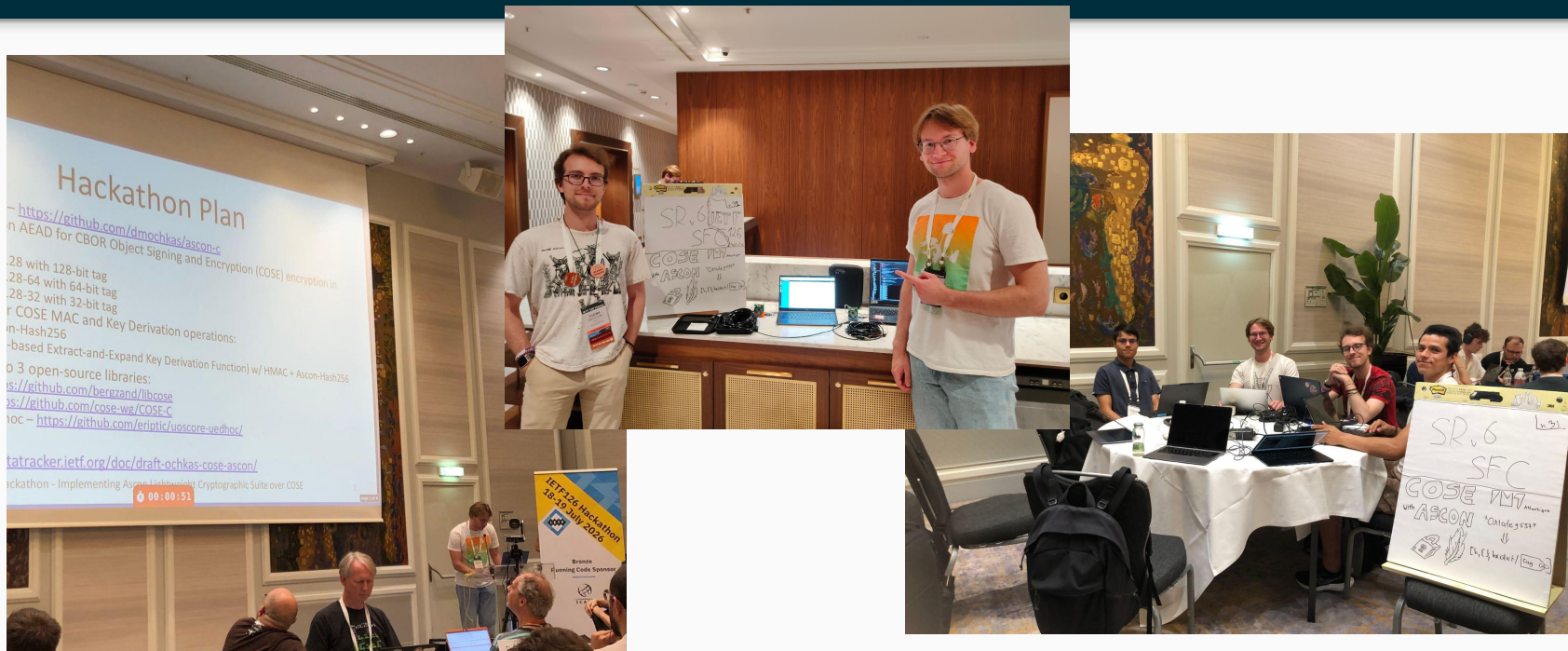
Evolution of the draft

- Key Derivation and MAC with Ascon-Hash256.
- 2 new algorithms for COSE MAC:
 - HMAC with Ascon-Hash256 (**HMAC-Ascon**).
 - **HMAC-Ascon/64** with output truncated to 64 bits.
- New Key Derivation algorithm – **HKDF with HMAC-Ascon**.
- **direct+HKDF-Ascon-Hash256**.

TODO list for full Ascon integration

- ✓ Ascon-AEAD128 for COSE encryption
- ✓ Ascon-AEAD128-64 for COSE encryption
- ✓ Ascon-AEAD128-32 for COSE encryption
- ✓ HMAC Ascon-Hash256 for COSE MAC
- ✓ HMAC Ascon-Hash256/64 for COSE MAC
- ✓ HKDF Ascon-Hash256 for Key Derivation
- ✓ direct+HKDF-Ascon-Hash256
- ✗ ECDH-ES+HKDF-Ascon-Hash256
- ✗ ECDH-SS+HKDF-Ascon-Hash256
- ✗ Ascon-Hash256 (RFC 9054)

Hackathon



<https://wiki.ietf.org/en/meeting/126/hackathon#implementing-ascon-lightweight-cryptographic-suite-over-cose>

Hackathon

- Fork & Pull Request to libcose (<https://github.com/bergzand/libcose/pull/132>):
 - ✓ Ascon-AEAD128 w/ 128-bit, 64-bit, and 32-bit tags
 - ✓ HMAC w/ Ascon-Hash256 (HMAC-Ascon)
 - ✓ HKDF w/ HMAC-Ascon
- Fork & Pull Request to COSE-C (<https://github.com/cose-wg/COSE-C/pull/142>):
 - ✓ Ascon-AEAD128 w/ 128-bit, 64-bit, and 32-bit tags
 - ✗ HMAC-Ascon
 - ✗ HKDF w/ HMAC-Ascon
- Fork of uoscore-uedhoc (<https://github.com/dmochkas/uoscore-uedhoc>):
 - ✓ Ascon-AEAD128 w/ 128-bit, 64-bit, and 32-bit tags
 - ✓ HMAC-Ascon
 - ✓ HKDF w/ HMAC-Ascon

References

<https://datatracker.ietf.org/doc/draft-ochkas-cose-ascon/>

<https://github.com/dmochkas/ascon-c>

<https://datatracker.ietf.org/doc/rfc9052>

<https://datatracker.ietf.org/doc/rfc9053>

<https://datatracker.ietf.org/doc/rfc9054>

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-232.pdf>

<https://wiki.ietf.org/en/meeting/126/hackathon#implementing-ascon-light-weight-cryptographic-suite-over-cose>

<https://github.com/dmochkas/ascon-c>

<https://github.com/dmochkas/libcose>

<https://github.com/dmochkas/COSE-C>

<https://github.com/dmochkas/uoscore-uedhoc>

Let's discuss



draft-ochkas-cose-ascon