IOAM / POT

SFC WG

November 8th, 2018

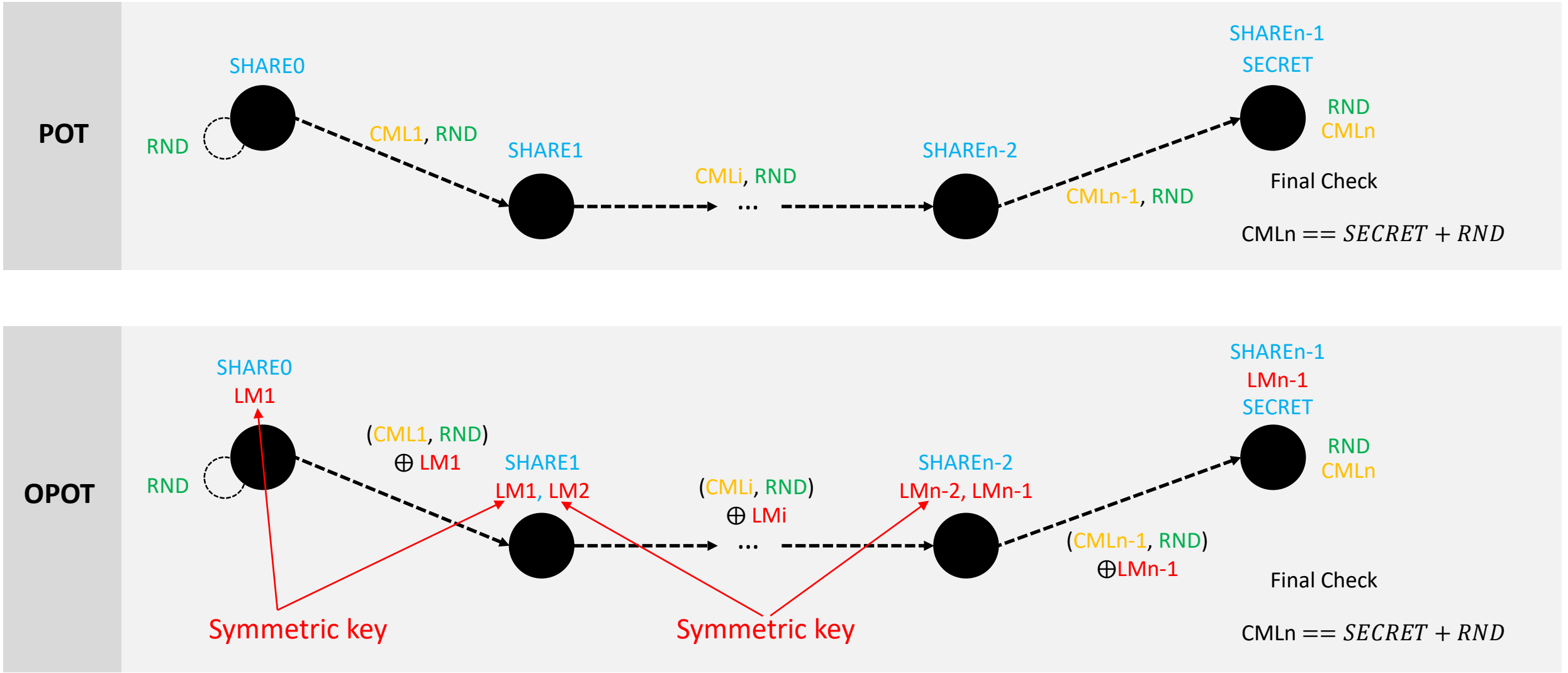
draft-ietf-sfc-ioam-nsh

- No comments received on draft.
  No changes to draft-ietf-sfc-ioam-nsh-00 since last SFC WG meeting at IETF 102 in Montreal
- With a couple of editorial fixes, draft should be ready for WGLC.

draft-ietf-sfc-proof-of-transit-01

- Historically draft-ietf-sfc-proof-of-transit included 2 approaches:
  - SSSS based approach: Computationally lean, but did not offer order preservation (OPOT)
  - Nested Crypto based approach: Offers order preservation (OPOT), but with higher computational cost or need for hardware support
- Key change from -00 to -01: Ordered POT (OPOT) based on SSSS, per the discussion in SFC WG meeting at IETF 102 in Montreal
  - OPOT approach is algorithmically and operationally compatible with already documented SSSS-based POT

OPOT with SSSS (section 3.5.2)



draft-ietf-sfc-proof-of-transit-01 Evolution

- Discussion:
  Consolidate the two mechanisms (SSSS-based and nested-crypo-based). Document only SSSS-based approach with OPOT option (drop nested crypto approach from the document).

Next Steps

- draft-ietf-sfc-ioam-nsh – Document is stable.
  We will fix a couple of editorial nits and post a -01.
  Should we WGLC version -01?
- draft-ietf-sfc-proof-of-transit – WG decision: Single approach only?

Thank you