LISP PubSub

draft-ietf-lisp-pubsub-06

IETF 109 - Online

Changes since -05

- Removed the deployment assumption of pre-established security associations between ITRs and MSs

- Added mechanism to establish security associations via LISP-SEC
  - In a nutshell -> PubSubKey = KDF (OTK)

- PubSub nonce now kept per xTR-ID **+ EID-record**

SECDIR Early Review 1/2

- SECDIR review comments regarding nonces in LISP:

“The term ’nonce' seems to be used more as a ‘token’ [...] In one case it may be a random value, but in several others the value is stored, compared, and reused. This is inconsistent with the IETF's Security Glossary RFC 4949.”

- RFC 4949 definition of nonce:

“A random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing liveness and thus detecting and protecting against replay attacks.”

- What’s the WG view on this?

SECDIR Early Review 2/2

- SECDIR review comments regarding nonces in LISP :

“What to do when the value exceeds the field space?”

- Nonce field space = 2^64
- Assuming one PubSub update per second per xTR-ID per EID-Record
  - 60*60*24*365 = 31536000 new nonces per year
  - 2^64 / 31536000 = 584942417355 years to run out of nonces

Next Steps

- Does the WG believe that the document is ready for Last Call?