Encrypted IPv6 Performance and Diagnostic Metrics Version 2 (EPDMv2) Destination Option

draft-elkins-ippm-encrypted-pdmv2-02

Nalini Elkins: Inside Products: nalini.elkins@insidethestack.com

Michael Ackermann: BCBS Michigan: mackermann@bcbsm.com

Ameya Deshpande: NITK, Surathkal: ameyanrd@gmail.com

Tommaso Pecorella: University of Florence: tommaso.pecorella@unifi.it

Adnan Rashid: University of Florence: adnan.rashid@unifi.it

Where are we?

- Presented first at IETF 111 (had a side meeting)
- Again at IETF 112 (had a side meeting)
- Working on implementation (Linux kernel + API into user space, HPKE)
- Working on light-weight, general purpose registration protocol (demonstration at side meeting IETF 113)

Protocol Flow Summary: Registration

1. Primary client initiates a request to the primary server. The request contains a list of available ciphersuites for KEM, KDF,and AEAD.

2. Primary server responds to the primary client with one of the available ciphersuites and shares its public key.

3. Primary client generates a secret and its encapsulation. The primary client sends the encapsulation and a salt to the primary server. The salt is required during KDF in the Data Transfer phase.

4. Primary Server generates the secret with the help of the encapsulation and responds with a status message.

5. Primary server shares this key with secondary servers over TLS.

6. Primary client generates the client-specific secrets with the help of KDF by using the info parameter as the Client IP address. The primary client shares these keys with the corresponding secondary clients over TLS.

Ready for WG Adoption?

Thoughts?