Babel over DTLS

draft-ietf-babel-dtls-01

Antonin Decimo — antonin.decimo@gmail.com
David Schinazi — dschinazi.ietf@gmail.com
Juliusz Chroboczek — jch@irif.fr

Concept

- Use multicast Hellos to discover neighbors
- Establish DTLS connection
- Run all other TLVs inside DTLS
- More dependencies than HMAC but more features

Motivation

- Asymmetric keys
  - Granularity of trust
  - Revocation
- Confidentiality

Changes since -00

- DTLS connections have new server port (IANA TBD)
  - Initiated from ephemeral client port
- All TLVs except Multicast Hellos MUST be inside DTLS
  - Even IHU — simplifies security boundary
- Editorial changes to clarify document

Next Steps

- Working Group Last Call?