Distributed Keys with DNCP

Ted Lemon <ted.lemon@nominum.com>
Motivation

- Various services on the homenet might want to be secured with the following goals:
  - Limit which HNRs can participate in routing and naming
  - Identify which HNR is Doing Something Bad
  - (where "HNR" means something saying it's an HNR)
- Not clear that this is absolutely necessary
- But if we don't do it now, retrofitting it later is going to suck
Status quo

- HNCP offers key sharing
- Protocol isn't secure in any sense (DTLS is required, but it's not clear how that would work)
- Protocol is about picking a single "shared secret" key, not about identifying end nodes
- Not clear what use it is
Proposal

Each node generates a public/private keypair

Each node shares its public key

Every node has every other node's public key

Public keys can be used for DTLS or other public-key-based protocols

All the key does is establish that the node that published the public key is originating the traffic signed with the private key.
Conclusion...?

- I would like the working group to produce a specification for this, and am willing to write it
- Anyone interested in helping?