draft-williams-btns-00.txt

- IKE changes
- PAD/SPD changes
- Issues

Recap: IKE Changes

- IKE changes
  - No new bits on the wire
  - Nodes coerce unauthenticated peers' IDs to new ID type: public key ID
  - ID values: peers' public keys

Recap: PAD/SPD Changes

- PAD/SPD changes
  - For specifying when to accept BTNS
  - For specifying when to use unauthenticated credentials
  - 'UNKNOWN' (or whatever) ID selector value
    - As distinct from 'ANY'

Issues

- Is this the right approach?
- No support for non-BTNS peers with non-PK credentials
- Asymmetry

Issues: Asymmetry

- Asymmetry
  - BTNS-capable node **must** have creds that are acceptable to its non-BTNS peers, else → no asymmetry
  - Peers that don't send CERT
    - Apparently empty CERTREQ is OK, so use that to deal with peers that don't send CERT by default