Issue #36

Interaction of IKE_SA_INIT retransmissions with specific notifies

No replies yet

Issue #14

Bounding the retransmit time

This is possibly a change to the protocol, but it is also possibly a clarification that no one should expect the other party to keep the window open forever.

Issue #19

Motivation for including SPIs in the cookie

General agreement

Issue #62

Interaction of IKE_SA_INIT retransmissions with specific notifies

General agreement

Issue #16 and 45

Order of IKE payloads

General agreement that this can be demoted safely, but we should still hear from others.

Issue #11

Clarify which traffic selectors to use in rekeying

There is disagreement on what to do if the policy changes before the rekeying.

Issue #68

Counter mode ciphers in IKEv2 to protect IKE SA

Long discussion about IVs and the IKE SA