We'd like 5 minutes for each of two issues

see draft-spencer-ipsec-ike-implementation-01.txt

1) the meaning of "unique" re IKE message IDs

- we assert that they are ALL unique, never reused. This permits them to be remembered as a protection against replay attacks.

2) switch to new IPsec (phase 2) SAs immediately upon negotiation.

- this clears up the whole business of when new SAs are used.
- do not negotiate them before you need them.