RSA-AES-GCM TLS Ciphersuites

Joe Salowey

Abhijit Choudhury

David McGrew

draft-ietf-tls-rsa-aes-gcm-00

- Working towards alignment with ietf-tls-ecc-new-mac
  - Nonce text largely aligned
  - Some text on nonce management may need to move to TLS 1.2 spec
- Need to addition key exchange methods?
  - DSA?