- draft-newman-auth-scram-04.txt - revived from dead 1998 draft; editor is now Abhijit Menon-Sen
- Key SCRAM properties
  - Stored key is not plaintext equivalent
  - Random salt, iteration, server & client nonce, [server key], [TLS channel bindings], 2-3 round trips
  - No Realms, No Security Layer, Changing Userid does not invalidated StoredKey

SaltedPassword := H_i(HMAC(password, salt))

ClientKey := H(SaltedPassword)

StoredKey := H(ClientKey)

ClientSig := HMAC(StoredKey, Message)

ClientProof := ClientKey XOR ClientSig

ServerKey := HMAC(SaltedPassword, salt)

ServerSig := HMAC(ServerKey, Message)