AES-CCM Cipher Suites

Daniel Bailey (daniel.bailey@rsa.com)
Matthew Campagna (mcampagna@rim.com)
David McGrew (mcgrew@cisco.com)
Robert Dugal (rdugal@certicom.com)

draft-mcgrew-tls-aes-ccm-ecc-01

- Specifies the use of 4 new ciphersuites

```
TLS_ECDHE_ECDSA_WITH_AES_128_CCM = {TBD1,TBD1}
TLS_ECDHE_ECDSA_WITH_AES_256_CCM = {TBD2,TBD2}
TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 = {TBD3,TBD3}
TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 = {TBD4,TBD4}
```

- Similar to the GCM ECC cipher suites.
- Since Maastricht (IETF 78)
  - Changes for clients to use TLS client hello extensions (should be same as RFC 4492)
  - Analogous change that a server MUST support the use of these extensions

draft-mcgrew-tls-aes-ccm-01

- Specifies 16 new cipher suites of the form
  - RSA with and without DHE, with AES CCM using 128 and 256 bit block ciphers.
  - Pre-shared Key with and without DHE, with AES CCM using 128 and 256 bit block ciphers
- Updated draft contains very few differences from previous draft.
- Attempts made to reduce the number of suites by using default TLS 1.2 PRF
- Both drafts use the AEAD specifications from RFC 5116, and in TLS 1.2 (RFC 5246)

Proposal

- Accept these two drafts as TLS Working Group Items
  - ZigBee Smart Energy 2.0 is expecting to use these specifications and has done some initial interop testing
  - The Standards for Efficient Cryptography Group (SECG) will host a test server for the ECC algorithms at the existing interop site
    - Accessed via http://tls.secg.org