ERICSSON

ECDHE_PSK WITH AES-GCM AND AES-CCM

DRAFT-MATTSSON-TLS-ECDHE-PSK-AEAD-01

JOHN MATTSSON
DANIEL MIGAULT

BACKGROUND AND MOTIVATION

- Pre-Shared Key (PSK) Authentication is widely used in many scenarios.
  - 3GPP networks use pre-shared keys to authenticate both subscriber and network.
  - In IoT, PSK authentication is often preferred for energy efficiency reasons.
- Perfect Forward Secrecy (PFS) is a strongly recommended security feature
  - Can be accomplished using an ephemeral Diffie-Hellman key exchange method.
  - Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) provides PFS with excellent performance and small key sizes.
- AEAD algorithms are strongly recommended for security reasons.
  - AES-GCM and AES-CCM are the de facto standards.
- Problem: Cipher suites with ECDHE_PSK and AES-GCM or AES-CCM are not defined.

NEW ECDHE_PSK CIPHER SUITES

- The draft defines new ciphersuites combining ECDHE_PSK with AES-GCM and AES-CCM.
  - TLS_ECDHE_PSK_WITH_AES_128_GCM
  - TLS_ECDHE_PSK_WITH_AES_256_GCM
  - TLS_ECDHE_PSK_WITH_AES_128_CCM_8
  - TLS_ECDHE_PSK_WITH_AES_128_CCM
  - TLS_ECDHE_PSK_WITH_AES_256_CCM

- Two different key lengths (128 and 256 bit). One CCM cipher suite with truncated tag (64 bit) for use with constrained IoT devices.
- The cipher suites make use of the default TLS 1.2 Pseudorandom Function (PRF) and can only be used with TLS 1.2.

ERICSSON