Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman
2023-07-31

Recent community activity (thank you!)

Valerio Setti @Nordic

- Improve outcome-analysis.sh script
- driver-only ECC: BN.TLS testing
- PSA maximum size macro definitions should take support into account
- Driver-only ECC: TLS: rm uses of mbedtls_debug_print_mpi
- driver-only ECC: BN.x509 testing
- driver-only ECC: BN.PK testing
- TLS: Clean up ECDSA dependencies
- Define PSA_WANT_xxx_KEY_PAIR_yyy step 2/DH
- Define PSA_WANT_xxx_KEY_PAIR_yyy step 2/RSA
- TLS: Clean up (EC)DH dependencies
- driver-only ECC: EPCf.TLS testing

Tomi Fontanilles @Nordic

- Implement non-PSA pk_sign_ext()

Kusumit Ghoderao, Saketh Sunkishala @ Silicon Labs

- PBKDF2 CMAC implementation

Misc

- rsa_signature: Use heap memory to allocate DER encoded RSA private key - Sarvesh Bodakhe @espressif
- Fix doc on buffer requirements of GCM API - Chien Wong
- Fixed x509 certificate generation to conform to RFCs when using ECC key – marekjansta
- Comply with the received Record Size Limit extension - Kloolk
- asn1parse: Require minimal-length encodings of lengths - Demi-Marie Obenour

Major activities within core team

https://github.com/orgs/Mbed-TLS/projects/1

- Planning Mbed TLS 3.5 - September – October 2023
  - Size optimization (including driver-only ECP, bignum)
  - p-256m – reduce code size for SECP256R1 ECDH and ECDSA
- Planning Mbed TLS 3.6 LTS - end of 2023 (maybe early 2024)
  - TLS 1.3 early data, record size limit
  - PSA multi-threading support
  - Accessor functions for fields made private in 3.0
  - Driver-only cipher and AEAD
- Planning Mbed TLS 4.0 – mid 2024?
  - PSA_CRYPTO_C / CLIENT always on
  - Consume PSA-Crypto repository as source of PSA and crypto code
  - Remove some legacy interfaces & features

- PSA Crypto – prototyping move to separate repository
- Size optimization
  - This is a focus for Mbed TLS 3.5
- CI
  - Testing on Arm coming soon
- Review workload
  - Struggling for review bandwidth – any assistance from the community is hugely valuable
  - Easing the general review load accelerates progress on work prioritized by the community
  - Increased use of draft PRs