Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman
2023-03-27

Recent community activity (thank you!)

- Valerio Setti @ Nordic
  - Fix some MAX_SIZE macros when PSA ECC is accelerated
  - Avoid parse/unparsed public ECC keys in PK with USE_PSA
  - Driver-only EC J-PAKE testing (3x PRs)
  - Driver-only ECDH in TLS 1.2 (part 1)
  - Driver-only ECDH in TLS 1.2 (part 2)
  - Driver-only ECDH in TLS 1.3
  - Driver-only ECDSA, ECDH, ECJPAKE - support all accelerated
  - analyze_outcomes.py – usability enhancements

- Joakim Andersson @ Nordic
  - Fix dependency error in psa_key_derivation_abort
  - Fix dependency error in psa_key_derivation_output_key

- Kusumit Ghoderao @ Silicon Labs
  - Support for 8 byte nonce in ChaCha20 and ChaCha20-Poly1035

- Misc
  - X.509 – verify SAN IP address – G Strauss
  - LMS – reduce stack memory usage – M Fischer
  - TLS 1.3 ticket dependency fix – Norbert Fabritius
  - Threading impl for Windows – fwc-dc
  - Fix llvm warning – Sergey Nsk
  - Require minimal length ASN1 encoding – Demi Marie
  - Fix segfault in mbedtls_oid_get_numeric_string - Demi Marie
  - Adjust log level in DTLS - Mehmet Çağrı Aksoy

Major activities within core team

- Mbed TLS 3.4 coming tomorrow – March 28th
  - PKCS #7
  - PSA interruptible sign/verify
  - EC J-PAKE improvements
  - Performance
  - Code-size
  - Bug-fixes & security

- PSA Crypto – prototyping move to separate repository

- Driver-only hashes – functionally complete
- Driver-only ECC – in progress

- Historical review – items older than one year
  - Currently working through some old issues

- CI
  - OpenCI functional
  - Working on performance improvements

- 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