arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman
2023-06-19

© 2022 Arm

Recent community activity (thank you!)

Valerio Setti @Nordic

- Backport: crypto_config_test_driver_extension: handle PUBLIC_KEY the same way as KEY_PAIRs
- driver-only ECC: TLS: avoid use of mbedtls_ecp_write_key() (with USE_PSA)
- Driver-only ECC: auto-enable ECP_LIGHT when needed
- driver-only ECC: ECPf.PK testing

Kusumit Ghoderao, Saketh Sunkishala @ Silicon Labs

- PBKDF2: Out of range input cost
- Support for 8 byte nonce in ChaCha20 and ChaCha20-Poly1305

Demi Marie Obenour

- 16 PRs with updates to ASN.1 and x.509 code
- Mix of clean-up and stricter compliance

Misc

- Don't force _WIN32_WINNT values - Steve Lhomme
- Fixed x509 certificate generation to conform to RFCs when using ECC key - marekjansta
- ECP self test enhanced to use all Weierstrass curves when NIST optimization is enabled - Valentin Struchalin
- Support compilation using Clang on Windows – SlugFiller
- Fix error: comparison of integers of different signs: 'SOCKET' and 'int’ - SergioNSK
- Support parsing non-nul-terminated PEM strings - Koromix

EdDSA / SHA-3 - Pol Henarejos

- SHA-3 support
- Add support for EdDSA with ed25519 curve (pure ed25519, ed25519ctx and ed25519ph)

© 2022 Arm

Major activities within core team

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

- Planning Mbed TLS 3.5
  - September – October 2023
- Planning Mbed TLS 3.6, 4.0
- PSA Crypto – prototyping move to separate repository
- OPC-UA – various X.509 improvements
- Size optimization
  - Identified significant improvements in bignum, driver-only work, AES, constant-time
  - This is a focus for Mbed TLS 3.5
- Performance optimization
  - Various improvements to AES

- Driver-only ECC – in progress
- Historical review – PRs older than 3 months
  - SHA-3 merged
- 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
  - Increased use of draft PRs

© 2022 Arm