Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman

2023-07-03

© 2022 Arm

Recent community activity (thank you!)

- Valerio Setti @Nordic
  - PK: parse: fix disparity with private Montgomery keys
  - Define PSA_WANT_xxx_KEY_PAIR_yyy step 2/ECC
  - driver-only ECC: EPCf.TLS testing
  - driver-only ECC: ECPf.PK testing
  - driver-only ECC: EPCf.X509 testing
  - Driver-only ECC: auto-enable ECP_LIGHT when needed
  - driver-only ECC: TLS: avoid use of mbedtls_ecp_write_key() (with USE_PSA)
  - PK: refactor wrappers in the USE_PSA case
- Kusumit Ghoderao, Saketh Sunkishala @ Silicon Labs
  - PBKDF2 out of range input tests
  - PBKDF2 CMAC implementation
  - PBKDF2: Output bytes
- Misc
  - Fixed x509 certificate generation to conform to RFCs when using ECC key
  - Don't force _WIN32_WINNT values
  - aesce: do not specify an arch version when enabling crypto instructions
  - Add OID for Challenge Password
  - ssl: fix critical extension handling regression
  - Support compilation using CLang on Windows
  - Remove prompt to exit in all programs
  - Add a do-while loop around macros
  - x509parse tests: Replace TEST_ASSERT with TEST_EQUAL
- EdDSA / SHA-3 - Pol Henarejos
  - Add support for EdDSA with ed25519 curve (pure ed25519, ed25519ctx and ed25519ph)

© 2022 Arm
arm

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
  - 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

© 2022 Arm
arm