Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman

2023-07-17

Recent community activity (thank you!)

- Valerio Setti @Nordic
  - TLS: Clean up ECDSA dependencies
  - TLS: Clean up (EC)DH dependencies
  - Define PSA_WANT_xxx_KEY_PAIR_yyy step 2/DH
  - Define PSA_WANT_xxx_KEY_PAIR_yyy step 2/RSA
  - PK: parse: fix disparity with private Montgomery keys
  - 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
  - Fix order of steps in DTLS server example program – Daniel Mangum
  - aesce: use correct target attribute when building with clang - Beniamin Sandu
  - Don't force _WIN32_WINNT values – Steve LHomme
  - Added pragma to suppress warning at psa_set_key_domain_parameters – Pedro Cavalheiro
- Misc x.509
  - Support challenge password attribute in CSR – tijs
  - Fixed x509 certificate generation to conform to RFCs when using ECC key – marekjansta
  - asn1parse: Require minimal-length encodings of lengths – Demi Marie

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

arm