Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman

2023-04-24

Recent community activity (thank you!)

- Demi-Marie Obenour gains official reviewer status
- Valerio Setti @ Nordic
  - PK test cleanup
  - ECP dependencies in PK
  - Fix use of USE_PSA_INIT/DONE in test suites
  - Use pk_context pointer in PK
  - Avoid parse/unparse public ECC keys in PK with USE_PSA
  - Avoid parse/unparse private ECC keys in PK with USE_PSA
  - Driver-only ECP testing framework
  - PK: use PSA to complete public key when USE_PSA is enabled
  - Remove PSA_HAVE_FULL_xxx symbols
  - Define (private) "light" subset of ECP
  - PK tests: use PSA to generate keypairs when USE_PSA is enabled
  - driver-only ECDH: enable ECDH-based TLS 1.2 key exchanges -- part 2
  - PK: don't use mbedtls_ecp_check_pub_priv() when USE_PSA is enabled
  - Driver-only curves: parity starter
  - Some MAX_SIZE macros are too small when PSA ECC is accelerated
  - Improve analyze_outcomes.py script
  - Driver-only ECC: all three top-level modules
- Misc
  - TLS 1.3 session tickets dependency fix - Norbert Fabritius
  - CMake on OS X cleanup
  - Read and write RFC8410 (X25519 & X448) keys – Jethrogb
  - Record Size Limit extension (first step) – Kloolk
  - Update test cert to use AES instead of DES - Mukesh Bharsakle
  - Fix warning in ECDSA – Harshal5
  - Support challenge password attribute in CSR (RFC2985) – tisj
  - Added pragma to suppress warning at psa_set_key_domain_parameters – Pedro Cavalheiro
- Stephan Koch @Oberon
  - Fix PSA AEAD ChaCha20 test dependency
  - Fix derive_ecjpake_to_pms dependency in PSA crypto test
  - Fix expected export length for Edwards curves in test suite
  - Fix test to check output length on PSA_SUCCESS only
- Kusumit Ghoderao @ Silicon Labs
  - PBKDF2 input_integer
  - Support for 8 byte nonce in ChaCha20 and ChaCha20-Poly1035

arm

Major activities within core team

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

- Mbed TLS 3.4 released 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
- OPC-UA – various X.509 improvements
- AES improvements
  - Support AESCE with MSVC
  - Support accelerated implementation only
- Driver-only ECC – in progress
- Historical review – PRs older than 3 months
- 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

arm