Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman

2023-12-04

Recent community activity (thank you!)

Valerio Setti @Nordic

- merged: #7082 - driver-only ECDSA: add ssl-opt.sh testing with testing parity
- merged: #8540 - [G2] Make CCM and GCM work with the new block_cipher module
- merged: #8547 - [G2] Make PSA-AEAD work with cipher-light
- #8449 - Design discussion: add new symbol for PSA key enrollment functions
- #8521 - [G4] Make CTR-DRBG fall back on PSA when AES not built in
- #8579 - PK: clean up pkwrite
- #8590 - pkcs[5/12]: use cipher enums for encrypt and decrypt

SiLabs

- #8198 silabs-Kusumit - KDF incorrect initial capacity

Misc

- merged: #8546 BrianX7c - [cipher.h] Arithmetic overflow in binary left shift operation
- merged: #5501 gstrauss - Add mbedtls_ssl_ticket_rotate() for ticket rotation
- merged: #8515 mschulz-at-hilscher - Fix compiler error on gcc 4.5.2.
- #7214 DemiMarie - asn1parse: Require minimal-length encodings of lengths
- #8321 irwir - Restore Windows XP platform support
- #7977 ivq - Fix doc on GCM API
- #7455 KloolK - Comply with the received Record Size Limit extension
- #8481 michael2012z - Remove transparent key check in psa_asymmetric_encrypt/decrypto()
- #8511 mschulz-at-hilscher - Add benchmark for RSA 3072
- #8510 mschulz-at-hilscher - Add LMS benchmark
- #8512 mschulz-at-hilscher - Alternative Timing compatible benchmark.c
- #8513 mschulz-at-hilscher - Explicitly accessing private fields in benchmark
- #8514 mschulz-at-hilscher - Fix uninitialized variable warnings in ssl_msg.c
- #8563 Oldes - Fixed compilation for Haiku OS
- #7930 tomi-font - Implement non-PSA pk_sign_ext()

arm

Major activities within core team

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

- TF-PSA-Crypto
  - https://github.com/Mbed-TLS/TF-PSA-Crypto
  - Currently, read-only preview
  - Will become upstream source for crypto in Mbed TLS
- TLS 1.3 early data
  - In progress, continuing through Q1
- Driver-only cipher & AEAD
  - AES, GCM, CCM, ChachaPoly
- Thread-safe PSA
- Accessors for MBEDTLS_PRIVATE fields
  - Continue into Q1
- Planning Mbed TLS 4.0 – end 2024?
  - PSA_CRYPTO_C / CLIENT always on
  - Consume TF-PSA-Crypto repository as source of PSA and crypto code
  - Remove some legacy interfaces & features
- TF-PSA-Crypto – productization
- CI
  - Testing on Arm coming soon
- Planning Mbed TLS 3.6 LTS – Q1-Q2 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
  - Main focus for team in Q1

arm