Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath
2024-09-09

Recent community activity (thank you!)

- #9542 manoel-serafim - Performance Enhancements and Memory Footprint Reduction in mbedtls_internal_sha(256|512)_process_c()
- #9302 valeriosetti - PSA: use static key slots to store keys
- merged: #9529 jaimeMF - [Backport 2.28] tests: fix calloc() argument list (gcc-14 fix)
- #5824 polhenarejos - Add support to Ed448 in EdDSA
- #6556 polhenarejos - XChaCha20 and XChaCha20-Poly1305 support.
- #5823 polhenarejos - Add support for SHA-3 KMAC
- #5822 polhenarejos - SHA-3 cSHAKE128 and cSHAKE256 support
- #5821 polhenarejos - SHA-3 SHAKE128 and SHAKE256 support
- #5819 polhenarejos - Add support for EdDSA with ed25519 curve (pure ed25519, ed25519ctx and ed25519ph)
- #9423 BhanuPrakash-P - Fix pkcs8 unencrypted private key parsing with Attributes field
- #9294 juhaylinen - Disable allow_abbrev from Python scripts using argparse
- #9001 raymo200915 - Add PKCS#7 parser features for integrating MbedTLS with U-Boot
- #8800 winterheart - Allow install headers to different location (mbedtls-3)
- merged: #9486 sergio-nsk - [Backport 3.6] Fix Mbed-TLS build when WIN32_LEAN_AND_MEAN macro is defined globally
- merged: #9485 sergio-nsk - Fix Mbed-TLS build when WIN32_LEAN_AND_MEAN macro is defined globally
- #9489 rsaxvc - Optimize software gcm_mult() routines on strictly-aligned systems
- #9218 casaroli - Make local functions and objects static

Major activities within core team

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

- TF-PSA-Crypto — main focus in Q3
  - Splitting files, reworking some interfaces (configuration, platform, …)
  - https://github.com/Mbed-TLS/TF-PSA-Crypto
  - Will become upstream source for crypto in Mbed TLS
- Mbed TLS 4.0
  - PSA_CRYPTO_C / CLIENT always on
  - Consume TF-PSA-Crypto repository as source of PSA and crypto code
  - Remove some legacy interfaces & features
- Mbed TLS 3.6.1
  - Focus on regressions in 3.6.0
  - Workarounds for TLS 1.3 issues: https://github.com/Mbed-TLS/mbedtls/issues/9210#issuecomment-2141498918
- Open for SPAKE2+ reviews (tasks defined on backlog board)

Release Timeline

- 3.6.1 released
- 4.0 currently aiming for first half of 2025
- 3.6 LTS supported until early 2027
- 2.28 LTS ends supported life end of 2024

TF-PSA-Crypto 1.0 + Mbed TLS 4.0 highlights

- TLS 1.2: removing finite-field DH, static ECDH, PKCS#1v1.5 RSA encryption, CBC
- Crypto: removing PKCS#1v1.5 RSA encryption, DES, EC curves smaller than 250 bits
- Removing all crypto ALT (use PSA drivers instead)
- Removing low-level crypto APIs (use PSA APIs instead)
  - Removing cipher.h; Keeping parts of md.h and pk.h partially as transition layers
  - Removing direct access to bignum/ECC arithmetic
  - Removing direct access to DRBG

Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה
ధన్యవాదములు