Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Gilles Peskine

2025-11-03

Recent community activity (thank you!)

- tls#10489 zacharykeyessonos - Fix module-import-in-extern-c compiler error (3.6)
- tls#10488 zacharykeyessonos - Fix module-import-in-extern-c compiler error
- merged: tls#10477 Cube707 - add cast to fix IAR compiler errors
- merged: tls#10478 Cube707 - [backport] add cast to fix IAR compiler errors
- tls#10485 lanodan - timing: replace deprecated gettimeofday() with clock()
- tls#10457 HaniAmmar - Add functions to export TLS traffic keys and sequence numbers for KTLS integration
- merged: tls#10470 Begasus - Use GNUInstallDirs CMAKE_INSTALL_INCLUDEDIR path for headers installation
- merged: tls#10469 Begasus - Use GNUInstallDirs CMAKE_INSTALL_INCLUDEDDIR path for headers installation
- tls#10270 Cube707 - add cast to fix IAR compiler warnings
- tls#10433 Mario-Klebsch - Increased MBEDTLS_BEFORE_COLON (size of temporary buffer) to 32
- tls#10463 lukaszobernig - Add ML-DSA-87 signature scheme implementation, based on BoringSSL.
- merged: tls#317 jleroy - cert_write : fix "Destination buffer is too small" error
- merged: frame#228 ruiliio - AES-XTS: update test generation for double-size key handling
- frame#230 TakutoYamane - fix: correct spelling of received in log messages
- crypto#557 zacharykeyessonos - Fix module-import-in-extern-c compiler error
- merged: crypto#547 Begasus - Use GNUIstalldir CMAKE_INSTALL_INCLUDEDIR for headers installation
- merged: crypto#159 daverodgman - Neon impl of ChaCha20 (better size & perf)
- crypto#494 amjoul01 - Expand mbedtls_to_psa_error to LMS
- crypto#538 ruiliio - Add support for AES-XTS

Recent community activity (thank you!)

Valerio @Nordic

- tls#10473 valeriosetti - [3.6] psa_load_builtin_key_into_slot: prevent accessing the PSA storage if key ID is in volatile range
- tls#10475 valeriosetti - [mbedtls] psa_load_builtin_key_into_slot: prevent accessing the PSA storage if key ID is in volatile range [1/2]
- merged: tls#10447 valeriosetti - [3.6] psa: improve buffer size computation for static key slots
- frame#223 valeriosetti - tests: migrate tests using secp192[k|r]1 toward secp256[r|k]1 --> PK [1/2]
- crypto#492 valeriosetti - [tf-psa-crypto] psa_load_builtin_key_into_slot: prevent accessing the PSA storage if key ID is in volatile range
- merged: crypto#496 valeriosetti - PK: remove `pk_context::pk_ctx`
- merged: crypto#460 valeriosetti - [tf-psa-crypto] Align header include guards with their new locations in TF PSA Crypto
- crypto#513 valeriosetti - tests: migrate tests using secp192[k|r]1 toward secp256[r|k]1 --> PK [2/2]
- merged: crypto#497 valeriosetti - Remove the RSA key mutex
- merged: crypto#498 valeriosetti - PK: fix config dependencies and simplify guards
- merged: crypto#528 valeriosetti - [tf-psa-crypto] psa: improve buffer size computation for static key slots

Major activities within core team

https://github.com/orgs/Mbed-TLS/projects/18

- Mbed TLS 4.0/TF-PSA-Crypto 1.0 bugfixes
- PK module refactoring
- Cleanups after legacy API removals
- Moving driver tests to Crypto CI
- Release automation
- Investigating ML-DSA integration

Release Timeline

- 1.x/4.x
  - 1.0/4.0 (Oct 2025 – released): New major version
  - 1.1/4.1 (TBD)
- 3.6 LTS supported until early 2027
  - 3.6.5 (Oct 2025 - released): Security fixes and bugfixes
  - 3.6.6 (TBD)

arm

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