arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2025-11-17

Recent community activity (thank you!)

- tls#10492 jbsgh - [3.6] Pr for issue 10434
- merged: tls#10496 JuhaPekkaa - Update log level for mbedtls_ssl_check_record and PSA-based ECDH computation
- merged: tls#10497 JuhaPekkaa - Update log level for mbedtls_ssl_check_record and PSA-based ECDH computation (3.6)
- tls#10485 lanodan - timing: replace deprecated gettimeofday() with clock()
- tls#10488 zacharykeyessonos - Fix module-import-in-extern-c compiler error
- tls#10489 zacharykeyessonos - Fix module-import-in-extern-c compiler error (3.6)
- merged: tls#10477 Cube707 - add cast to fix IAR compiler errors
- merged: tls#10478 Cube707 - [backport] add cast to fix IAR compiler errors
- frame#230 TakutoYamane - fix: correct spelling of received in log messages
- crypto#573 mfil - Use instruction-level parallelism with AES-NI to speed up AES-CTR
- crypto#538 ruiliio - Add support for AES-XTS·
- crypto#563 ivv19041994 - fix memory sanitize for AES-NI
- crypto#557 zacharykeyessonos - Fix module-import-in-extern-c compiler error

Recent community activity (thank you!)

Valerio @Nordic

- tls#10499 valeriosetti - [shadow] Testing of crypto#564
- tls#10505 valeriosetti - Remove use of `pk_can_do()`
- merged: tls#10498 valeriosetti - [mbedtls] tests: migrate tests using secp192[k|r]1 toward secp256[r|k]1 --> EC [2/3]
- merged: tls#10473 valeriosetti - [3.6] psa_load_builtin_key_into_slot: prevent accessing the PSA storage if key ID is in volatile range
- tls#10495 valeriosetti - [mbedtls] Remove dead code in RSA [2/3]
- merged: tls#10491 valeriosetti - Remove temporary fixes introduced in #10213
- merged: frame#235 valeriosetti - [framework] tests: migrate tests using secp192[k|r]1 toward secp256[r|k]1 --> EC [1/3]
- merged: frame#223 valeriosetti - tests: migrate tests using secp192[k|r]1 toward secp256[r|k]1 --> PK [1/2]
- frame#234 valeriosetti - [framework] Remove dead code in RSA [1/3]
- crypto#564 valeriosetti - [tf-psa-crypto] tests: migrate tests using secp192[k|r]1 toward secp256[r|k]1 --> EC [3/3]
- crypto#572 valeriosetti - Add new test components with different combinations of PKPARSE and PKWRITE
- crypto#565 valeriosetti - [tf-psa-crypto] tests: migrate tests using secp192[k|r]1 toward secp256[r|k]1 --> PSA
- merged: crypto#492 valeriosetti - [tf-psa-crypto] psa_load_builtin_key_into_slot: prevent accessing the PSA storage if key ID is in volatile range
- crypto#570 valeriosetti - Remove suport for secp192[k|r]1 curves
- crypto#559 valeriosetti - Remove dead code in RSA
- merged: crypto#513 valeriosetti - tests: migrate tests using secp192[k|r]1 toward secp256[r|k]1 --> PK [2/2]

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)

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