arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2025-12-15

Recent community activity (thank you!)

- merged: tls#10157 jadaber - Remove use of mbedtls_md_get_name() from ssl_context_info.c
- tls#10514 ng-gsmk - mbedtls_ssl_get_alert(): getter for fatal alerts
- tls#10457 HaniAmmar - Add functions to export TLS traffic keys and sequence numbers for KTLS integration
- tls#10431 rgqsch - Add challenge password to CSR Development
- tls#8246 lpy4105 - Refine the command for generating library in tests and programs
- crypto#583 daverodgman - chacha20 - further size and perf improvements
- crypto#588 kusumitg - Add psa_pake_set_context function for spake2p

Recent community activity (thank you!)

Valerio @Nordic

- tls#10539 valeriosetti - Remove temporary fix for secp192 curves in `test_psa_crypto_without_heap`
- tls#10517 valeriosetti - Remove use of pk_debug()
- merged: tls#10505 valeriosetti - Remove use of `pk_can_do()`
- merged: tls#10522 valeriosetti - [mbedtls] Remove support for secp192[k|r]1 curves (part 2)
- merged: frame#247 valeriosetti - Remove dirty fix for secp192 curves added in #570
- merged: frame#242 valeriosetti - [framework] Remove support for secp192[k|r]1 curves
- crypto#577 valeriosetti - PK: add `mbedtls_pk_write_pubkey_psa()`
- merged: crypto#595 valeriosetti - Remove dirty fix for secp192 curves added in #570
- crypto#600 valeriosetti - tests: pk: add a common function to create a PSA key out of predefined keys
- merged: crypto#570 valeriosetti - Remove support for secp192[k|r]1 curves

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