arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2025-12-01

Recent community activity (thank you!)

- tltls#10514 ng-gsmk - mbedtls_ssl_get_alert(): getter for fatal alerts
- tls#10086 jurassicLizard - fix MBEDTLS_CONFIG_FILE not installing properly
- tls#10084 jurassicLizard - [Backport 3.6] add handling for default CMAKE_BUILD_TYPE values
- tls#10079 jurassicLizard - [development] introduce handling for default CMake Build types
- tls#10510 kanren3 - Reject high-tag-number ASN.1 tags in mbedtls_asn1_get_tag()
- frame#241 neeraj9 - Use sys.executable for script execution to respect virtual environment
- crypto#581 nicola-mazzucato-arm - psa: Reorganise values of PSA_ERROR_
- crypto#573 mfil - Use instruction-level parallelism with AES-NI to speed up AES-CTR
- crypto#222 jurassicLizard - add handling for default CMAKE_BUILD_TYPE values

Recent community activity (thank you!)

Valerio @Nordic

- tls#10522 valeriosetti - [mbedtls] Remove support for secp192[k|r]1 curves (part 2)
- merged: tls#10519 valeriosetti - [mbedtls] Remove support for secp192[k|r]1 curves
- tls#10517 valeriosetti - Remove use of pk_debug()
- frame#242 valeriosetti - [framework] Remove support for secp192[k|r]1 curves
- crypto#570 valeriosetti - Remove support for secp192[k|r]1 curves
- crypto#577 valeriosetti - PK: add `mbedtls_pk_write_pubkey_psa()`
- merged: crypto#559 valeriosetti - Remove dead code in RSA
- merged: crypto#572 valeriosetti - Add new test components with different combinations of PKPARSE and PKWRITE
- merged: crypto#565 valeriosetti - [tf-psa-crypto] tests: migrate tests using secp192[k|r]1 toward secp256[r|k]1 --> PSA
- merged: crypto#564 valeriosetti - [tf-psa-crypto] tests: migrate tests using secp192[k|r]1 toward secp256[r|k]1 --> EC [3/3]

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