# Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath, Gilles Peskine

2026-01-26

# Recent community activity (thank you!)

- tls#10572 machine-moon - Fix MinGW printf ll macro
- tls#10557 frankencode - Fix: support empty PSK key hint in Client Key Exchange message
- tls#10514 ng-gsmk - mbedtls_ssl_get_alert(): getter for fatal alerts
- tls#10558 frankencode - [3.6] Fix: support empty PSK key hint in Client Key Exchange message
- tls#6192 greg3844 - Fix CRL with critical extension can't be loaded
- tls#5967 mprse - Refactor key derivation structure for the driver interface + Implement key derivation input getters v.2
- tls#10553 dc6jgk - allow negotiation of all use_srtp profile values currently listed by IANA
- tls#10457 HaniAmmar - Add functions to export TLS traffic keys and sequence numbers for KTLS integration
- frame#241 neeraj9 - Use sys.executable for script execution to respect virtual environment
- crypto#664 daverodgman - AES performance
- crypto#425 ilie-halip-nxp - scripts: driver_templates: fix few driver wrappers
- crypto#583 daverodgman - chacha20 - further size and perf improvements
- crypto#538 ruiliio - Add support for AES-XTS·
- crypto#649 daverodgman - fix error in GCC bswap

# Recent community activity (thank you!)

## Valerio @Nordic

- tls#10570 valeriosetti - mbedtls 4.x does not expose mbedtls_ecp_curve_list()
- merged: tls#10564 valeriosetti - Remove unused script `set_psa_test_dependencies.py`
- merged: tls#10559 valeriosetti - tests: scripts: configuration-crypto: fix paths for "not grep"
- merged: tls#10517 valeriosetti - Remove use of pk_debug()
- merged: frame#257 valeriosetti - [framework] tests: pk: add a common function to create a PSA key out of predefined keys
- crypto#673 valeriosetti - Only build mbedtls_rsa_deduce_private_exponent when key generation is enabled
- merged: crypto#600 valeriosetti - [tf-psa-crypto] tests: pk: add a common function to create a PSA key out of predefined keys
- merged: crypto#666 valeriosetti - Stop defining inline in our headers
- crypto#668 valeriosetti - Software GCM table calculation buggy with gcc -O3
- merged: crypto#661 valeriosetti - Use MPI functions to fill RSA contexts in tests for RSA export
- merged: crypto#659 valeriosetti - Remove residual uses of MBEDTLS_ECDSA_DETERMINISTIC
- merged: crypto#617 valeriosetti - PK: remove pk_debug() and related stuff

# Major activities within core team

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

- Mbed TLS 4.1/TF-PSA-Crypto 1.1 preparations
- PK module refactoring
- Prototyping and starting ML-DSA integration
- Bug bounty program
- Code size optimization initial investigation

# Release Timeline

- 1.x/4.x
  - 1.0/4.0 (Oct 2025 – released): New major version
  - 1.1/4.1 (planned for end of March 2026): new LTS version
- 3.6 LTS supported until early 2027
  - 3.6.5 (Oct 2025 - released): Security fixes and bugfixes
  - 3.6.6 (planned for end of March 2026)

arm

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