arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2026-07-13

Recent community activity (thank you!)

Mbed TLS

- tls#10791 nvxbug - Reject out-of-bounds session ID length in ssl_tls12_session_load
- tls#10792 nvxbug - Reject out-of-bounds ALPN length in ssl_context_load
- tls#10809 abtom87 - library/ssl_tls13_keys: exit immediately upon failure.
- tls#10457 HaniAmmar - Add functions to export TLS traffic keys and sequence numbers for KTLS integration
- tls#10553 dc6jgk - allow negotiation of all use_srtp profile values currently listed by IANA
- tls#10782 abtom87 - scripts: scan tf-psa-crypto/include/mbedtls for error codes
- tls#10813 abtom87 - ssl_tls13_server: validate supported_versions extension length
- tls#10807 crabel99 - Async hardware cryptographic function support
- tls#10801 Old-Ding - ssl: remove impossible signature algorithm null check
- tls#10802 Old-Ding - ssl: remove impossible signature algorithm null check
- tls#10794 Old-Ding - ssl: remove impossible signature algorithm null check
- tls#10800 michaelsam94 - Clarify CRL validity flags for multiple CRLs
- tls#10793 DragonBluep - [mbedtls-3.6] fix arm32 build errors with GCC 15.3
- merged: tls#10731 AmyChan-Intel - library/alignment.h: Fix 'MBEDTLS_GCC_VERSION' is not defined error
- tls#10752 erorndev - ssl: reject trailing bytes in TLS 1.3 encrypted extensions
- tls#10783 abtom87 - mbedtls/ssl.h: ssl_user_data_* accepts const pointers.

Recent community activity (thank you!)

TF-PSA Crypto

- frame#307 asmellby - scripts: Add dispatch include path and new generation location
- merged: frame#301 OldManYellsAtCloud - c_build_helper: Split cc command line
- crypto#538 ruiliio - Add support for AES-XTS·
- crypto#809 asmellby - Complete the move of driver wrappers to the dispatch/ directory
- crypto#720 parmi93 - Remove pattern constraint from location field
- crypto#730 hasheddan - docs: fix broken links between specifications
- crypto#829 crabel99 - Async hardware cryptographic function support·
- merged: crypto#800 AmyChan-Intel - core/alignment.h: Fix 'MBEDTLS_GCC_VERSION' is not defined error
- merged: crypto#801 AmyChan-Intel - 1.1: core/alignment.h: Fix 'MBEDTLS_GCC_VERSION' is not defined error
- crypto#819 sigvartmh - SPAKE2+: Prover key pair import and export
- crypto#818 sigvartmh - SPAKE2+: Add psa_pake_set_context function for SPAKE2+

Recent community activity (thank you!)

Valerio (Nordic)

- tls#10814 valeriosetti - Reduce dependencies on private `ecp.h` header
- tls#10804 valeriosetti - pk: improve error code failure reporting when RSA public key parsing fails (1/2)
- tls#10764 valeriosetti - Allow TF-PSA-Crypto path to be specified in CMake and Makefiles
- tls#10642 valeriosetti - Replace legacy rsa symbols followup
- crypto#827 valeriosetti - pk: improve error code failure reporting when RSA public key parsing fails (2/2)

Major activities within core team

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

- ML-DSA integration
  - Priority to bootloader/firmware use cases
- Bug bounty program

Release Timeline

- 1.x/4.x development
  - 1.2/4.2 released on 2026-07-07
- 1.1.x/4.1.x LTS supported until March 2029
  - 1.1.0/4.1.0 released on 2026-03-31
  - 1.1.1/4.1.1 released on 2026-07-07
- 3.6 LTS supported until early 2027
  - 3.6.7 released on 2026-07-07
  - 3.6.6 (2026-03-31): Security fixes and bugfixes

arm

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