arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2026-06-29

Recent community activity (thank you!)

Mbed TLS

- tls#10794 Old-Ding - ssl: remove impossible signature algorithm null check
- tls#10793 DragonBluep - [mbedtls-3.6] fix arm32 build errors with GCC 15.3
- 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.
- tls#10792 nvxbug - Reject out-of-bounds ALPN length in ssl_context_load
- tls#10791 nvxbug - Reject out-of-bounds session ID length in ssl_tls12_session_load
- tls#10714 lhuang04 - Add MBEDTLS_SSL_TLS_HS_LARGE_MSG for large handshake message reassembly
- tls#10731 AmyChan-Intel - library/alignment.h: Fix 'MBEDTLS_GCC_VERSION' is not defined error
- tls#10782 abtom87 - scripts: scan tf-psa-crypto/include/mbedtls for error codes
- tls#10780 asmellby - Complete the move of TF-PSA-Crypto driver wrappers to dispatch/ directory
- merged: tls#10761 Nadav0077 - Backport to 4.1: harden serialized data deserialization
- merged: tls#10762 Nadav0077 - Backport to 3.6: harden serialized data deserialization
- merged: tls#10715 Nadav0077 - Harden TLS 1.3 serialized session loading
- tls#10777 plusky - cmake: install libmbedcrypto compat library as a program
- tls#10778 ThePassionate - Fix TriCore MULADDC clobber list missing carry register
- tls#10776 MathisMARION - Fix generate_features.pl for X.509 section

Recent community activity (thank you!)

TF-PSA Crypto

- test#257 saheerb - Throttle large parallel fan-out with throttle categoy
- frame#307 asmellby - scripts: Add dispatch include path and new generation location
- frame#308 sigvartmh - Add Spake2p support to test framework
- crypto#819 sigvartmh - SPAKE2+: Prover key pair import and export
- crypto#818 sigvartmh - SPAKE2+: Add psa_pake_set_context function for SPAKE2+
- crypto#820 sigvartmh - SPAKE2+: Add prover setup and key-share output for SPAKE2+
- crypto#817 sigvartmh - SPAKE2+: Implement public key import and export
- crypto#809 asmellby - Complete the move of driver wrappers to the dispatch/ directory
- crypto#801 AmyChan-Intel - 1.1: core/alignment.h: Fix 'MBEDTLS_GCC_VERSION' is not defined error
- crypto#800 AmyChan-Intel - core/alignment.h: Fix 'MBEDTLS_GCC_VERSION' is not defined error
- crypto#815 sigvartmh - SPAKE2+: Implement psa_pake_set_context()
- crypto#810 sigvartmh - SPAKE2+ PSA PAKE API support

Recent community activity (thank you!)

Valerio (Nordic)

- test#257 saheerb - Throttle large parallel fan-out with throttle categoy
- frame#307 asmellby - scripts: Add dispatch include path and new generation location
- frame#308 sigvartmh - Add Spake2p support to test framework
- crypto#819 sigvartmh - SPAKE2+: Prover key pair import and export
- crypto#818 sigvartmh - SPAKE2+: Add psa_pake_set_context function for SPAKE2+
- crypto#820 sigvartmh - SPAKE2+: Add prover setup and key-share output for SPAKE2+
- crypto#817 sigvartmh - SPAKE2+: Implement public key import and export
- crypto#809 asmellby - Complete the move of driver wrappers to the dispatch/ directory
- crypto#801 AmyChan-Intel - 1.1: core/alignment.h: Fix 'MBEDTLS_GCC_VERSION' is not defined error
- crypto#800 AmyChan-Intel - core/alignment.h: Fix 'MBEDTLS_GCC_VERSION' is not defined error
- crypto#815 sigvartmh - SPAKE2+: Implement psa_pake_set_context()
- crypto#810 sigvartmh - SPAKE2+ PSA PAKE API support

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
- Mbed TLS 4.2/TF-PSA-Crypto 1.2 preparations
  - Minor improvements for driver integration

Release Timeline

- 1.x/4.x development
  - 1.2/4.2 aiming for early July
- 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 aiming for early July
- 3.6 LTS supported until early 2027
  - 3.6.7 aiming for early July
  - 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