arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath, Gilles Peskine

2026-05-04

Recent community activity (thank you!)

1/2

- tls#10731 AmyChan-Intel - library/alignment.h: Fix 'MBEDTLS_GCC_VERSION' is not defined error
- tls#10729 lhuang04 - Fix -Wundef warnings for PSA macros in pk_internal.h
- tls#10714 lhuang04 - Add MBEDTLS_SSL_TLS_HS_LARGE_MSG for large handshake message reassembly
- tls#10715 Nadav0077 - Harden TLS 1.3 serialized session loading
- tls#10717 lhuang04 - Fix -Wundef warnings for MBEDTLS_GCC_VERSION in alignment.h
- merged: tls#10695 valord577 - Fix build warning/error using llvm-mingw
- merged: tls#10711 valord577 - [backport 4.1 #10695] Fix build warning/error using llvm-mingw
- merged: tls#10202 LoveKarlsson - [3.6] Fix alignment problems with IAR and Zephyr
- tls#10730 AmyChan-Intel - library/alignment.h: Fix 'MBEDTLS_GCC_VERSION' is not defined error
- tls#10716 RedStar18 - Title: Add PSA Crypto minimal config and bootloader sources
- tls#9183 MaJerle - Remove unnecessary casting for return value of mbedtls_calloc
- merged: tls#10672 Maokaman1 - ssl: accept TLS 1.2 rsa_pss_rsae signature algorithms
- merged: tls#10674 Maokaman1 - Backport 3.6: ssl: accept TLS 1.2 rsa_pss_rsae signature algorithms
- merged: tls#10704 Maokaman1 - Backport 4.1: ssl: accept TLS 1.2 rsa_pss_rsae signature algorithms

Recent community activity (thank you!)

2/2

- frame#301 OldManYellsAtCloud - c_build_helper: Split cc command line
- frame#301 OldManYellsAtCloud - c_build_helper: Split cc command line
- frame#287 PLAJ-se - Add X.509 cert with rsassaPss key
- crypto#731 parmi93 - Fix PSA lifetime persistence argument
- crypto#782 lhuang04 - Fix -Wundef warnings for MBEDTLS_GCC_VERSION in alignment.h
- merged: crypto#779 LoveKarlsson - [1.1] Fix alignment problems with IAR and Zephyr
- merged: crypto#410 LoveKarlsson - Made alignment typedefs more robust for IAR
- crypto#778 Nadav0077 - Fix ML-DSA signing error propagation
- crypto#705 Marandil - Fix explicit Elliptic Curve parsing
- crypto#730 hasheddan - docs: fix broken links between specifications
- merged: crypto#743 M-Moawad - platform: fix -Wcast-align warnings in memory_buffer_alloc.c

Recent community activity (thank you!)

Valerio @Nordic

- tls#10642 valeriosetti - Replace legacy rsa symbols followup
- tls#10742 valeriosetti - [backport 4.1] mbedtls_config.c missing mbedtls_platform_requirements.h
- tls#10741 valeriosetti - mbedtls_config.c missing mbedtls_platform_requirements.h
- merged: tls#10713 valeriosetti - [backport 4.1] check_config: add missing check for TLS 1.3 key exchanges
- merged: tls#10650 valeriosetti - check_config: add missing check for TLS 1.3 key exchanges
- merged: tls#10712 valeriosetti - [backport 4.1] library: check_config: remove RSA encryption requirement from ECDHE-RSA
- merged: tls#10639 valeriosetti - library: check_config: remove RSA encryption requirement from ECDHE-RSA
- merged: tls#10692 valeriosetti - [backport 3.6] platform: fix -Wcast-align warnings in memory_buffer_alloc.c
- crypto#718 valeriosetti - doxygen: use CMake build dir intead of source dir to host generated files
- crypto#760 valeriosetti - [backport 1.1] doxygen: use CMake build dir intead of source dir to host generated files
- crypto#785 valeriosetti - [backport 1.1] include tf_psa_crypto_platform_requirements.h in tf_psa_crypto_config.c
- crypto#777 valeriosetti - include tf_psa_crypto_platform_requirements.h in tf_psa_crypto_config.c
- merged: crypto#757 valeriosetti - [backport 1.1] platform: fix -Wcast-align warnings in memory_buffer_alloc.c

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
- 1.1.x/4.1.x LTS supported until March 2029
  - 1.1.0/4.1.0 released on 2026-03-31
- 3.6 LTS supported until early 2027
  - 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