Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2026-07-27

Recent community activity (thank you!)

Mbed TLS

- tls#10839 dwivedys - x509:reject certificates with a zero serial number (RFC 5280)
- tls#10840 nzzlinh - Backport v3.6: Fix IAR endianness detection in alignment.h
- tls#10809 abtom87 - library/ssl_tls13_keys: exit immediately upon failure.
- tls#10829 mmustafasenoglu - Fix memory errors in sample programs
- tls#10793 DragonBluep - [mbedtls-3.6] fix arm32 build errors with GCC 15.3
- tls#10792 nvxbug - Reject out-of-bounds ALPN length in ssl_context_load
- tls#10833 nvxbug - Fix off-by-one over-read in TLS 1.2 ClientHello and CertificateRequest
- tls#10791 nvxbug - Reject out-of-bounds session ID length in ssl_tls12_session_load
- tls#10831 honma89 - Add input length validation in dummy_ticket_parse()
- tls#10828 ThePseudo - x509_crt: Add initialization to time `now`
- tls#10824 94xhn - Fix x509_get_uid() accepting constructed [1]/[2] tags
- tls#10827 94xhn - Fix x509_get_entries() not validating CRL entry's own SEQUENCE length is fully consumed
- tls#10826 94xhn - Reject zero-length serial number in mbedtls_x509write_crt
- tls#10825 94xhn - Reject empty ALPN protocol list in mbedtls_ssl_conf_alpn_protocols()
- tls#10489 zacharykeyessonos - Fix module-import-in-extern-c compiler error (3.6)
- tls#10488 zacharykeyessonos - Fix module-import-in-extern-c compiler error
- tls#10807 crabel99 - Async hardware cryptographic function support
- tls#10457 HaniAmmar - Add functions to export TLS traffic keys and sequence numbers for KTLS integration

Recent community activity (thank you!)

TF-PSA Crypto

- crypto#838 nzzlinh - Fix IAR compiler endianness detection in alignment.h
- crypto#837 krish2718 - docs: add WPA3-SAE (PSA Crypto API 1.4) design proposal
- crypto#841 Harshal5 - Fix XTS-AES in-place operation with partial final block
- crypto#844 abtom87 - pkcs5: reject iteration count of 0 in PBKDF2-HMAC
- crypto#845 nzzlinh - Backport 1.1: Fix IAR endianness detection in alignment.h
- crypto#843 okning - Fix getrandom detection with musl libc
- crypto#817 sigvartmh - SPAKE2+: Implement public key import and export
- crypto#820 sigvartmh - SPAKE2+: Add prover setup and key-share output for SPAKE2+
- crypto#819 sigvartmh - SPAKE2+: Prover key pair import and export
- crypto#810 sigvartmh - SPAKE2+ PSA PAKE API support
- crypto#818 sigvartmh - SPAKE2+: Add psa_pake_set_context function for SPAKE2+
- crypto#839 corelabtech - Merge
- crypto#538 ruiliio - Add support for AES-XTS
- crypto#557 zacharykeyessonos - Fix module-import-in-extern-c compiler error
- crypto#829 crabel99 - Async hardware cryptographic function support

Recent community activity (thank you!)

Valerio (Nordic)

- merged: 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#10814 valeriosetti - Reduce dependencies on private `ecp.h` header
- tls#10642 valeriosetti - Replace legacy rsa symbols followup
- crypto#673 valeriosetti - Only build mbedtls_rsa_deduce_private_exponent when key generation is enabled
- crypto#827 valeriosetti - pk: improve error code failure reporting when RSA public key parsing fails (2/2)
- crypto#811 valeriosetti - Inconsistent return value of mbedtls_pk_parse_key breaks mbedtls_pk_check_pair sometimes

Major activities within core team

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

- ML-DSA integration
  - Priority to bootloader/firmware use cases
- Investigation about adding SM3
- Bug bounty program

Release Timeline

- 1.x/4.x development
  - 1.2/4.2 released on 2026-07-07
  - 1.3/4.3 targeted for end of September
- 1.1.x/4.1.x LTS supported until March 2029
  - 1.1.1/4.1.1 released on 2026-07-07
  - 1.1.2/4.1.2 targeted for end of September
- 3.6 LTS supported until early 2027
  - 3.6.7 released on 2026-07-07
  - 3.6.8 targeted for end of September

arm

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