Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath, Gilles Peskine

2026-03-23

Recent community activity (thank you!)

- tls#10646 rado17 - Add support for wildcard hostname checks
- tls#10616 nandojve - x509: Parse all certificate policy OIDs per RFC 5280
- tls#10631 yiwu0b11 - Support DESTDIR for install and add build-system test
- tls#10637 yiwu0b11 - Backport 3.6: tests: add CMake DESTDIR install coverage in components-build-system
- tls#10632 PLAJ-se - rsa: support parsing RSASSA-PSS keys
- tls#10633 PLAJ-se - pk: (backport 3.6): add support for RSASSA-PSS in mbedtls_pk_parse_subpubkey
- tls#10572 machine-moon - Fix MinGW printf ll macro
- frame#285 Marandil - Add explicit parameter variants to ec_*_pub data files
- frame#287 PLAJ-se - Add X.509 cert with rsassaPss key
- crypto#723 aescolar - psa_crypto.c: Fix ifdefs to avoid build warning
- crypto#720 parmi93 - Remove pattern constraint from location field
- crypto#705 Marandil - Fix explicit Elliptic Curve parsing
- crypto#625 cxx194832 - SHA256 performance optimized by RVV
- merged: crypto#710 adeaarm - psa: parenthesize truncation test in PSA_MAC_LENGTH
- crypto#706 PLAJ-se - builtin: add support for RSASSA-PSS in mbedtls_pk_parse_subpubkey
- crypto#538 ruiliio - Add support for AES-XTS

Recent community activity (thank you!)

Valerio @Nordic

- tls#10639 valeriosetti - library: check_config: remove RSA encryption requirement from ECDHE-RSA
- merged: tls#10591 valeriosetti - library: replace `MBEDTLS_RSA_C` with `PSA_WANT`
- tls#10642 valeriosetti - Replace legacy rsa symbols followup
- merged: tls#10638 valeriosetti - library: x509: fix guard in mbedtls_x509_crt_profile_next
- crypto#718 valeriosetti - doxygen: use CMake build dir intead of source dir to host generated files

Major activities within core team

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

- Mbed TLS 4.1/TF-PSA-Crypto 1.1 preparations
  - Directory structure and build script improvements
  - Post-1.0 cleanup
  - …
- ML-DSA integration
- Bug bounty program
- Code size optimization initial investigation

Release Timeline

- 1.x/4.x development
- 1.1.x/4.1.x LTS supported until March 2029
  - 1.1.0/4.1.0 release planned for 31 March (tentative date)
  - Code freeze since 17 March
- 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)

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