Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath
2026-03-09

Recent community activity (thank you!)

- tls#10633 PLAJ-se - pk: (backport 3.6): add support for RSASSA-PSS in mbedtls_pk_parse_subpubkey
- tls#10632 PLAJ-se - rsa: support parsing RSASSA-PSS keys
- 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#10628 yiwu0b11 - Replace mbedtls_md_info_from_string() with strcmp()
- tls#10630 Marandil - Fix explicit Elliptic Curve parsing (3.6 backport)
- tls#10457 HaniAmmar - Add functions to export TLS traffic keys and sequence numbers for KTLS integration
- frame#287 PLAJ-se - Add X.509 cert with rsassaPss key
- frame#285 Marandil - Add explicit parameter variants to ec_*_pub data files
- crypto#706 PLAJ-se - builtin: add support for RSASSA-PSS in mbedtls_pk_parse_subpubkey
- crypto#705 Marandil - Fix explicit Elliptic Curve parsing
- crypto#702 daverodgman - AES-GCM size and perf
- crypto#538 ruiliio - Add support for AES-XTS
- tls#10591 valeriosetti - library: replace `MBEDTLS_RSA_C` with `PSA_WANT`
- merged: tls#10599 valeriosetti - [backport] include: fix guard in asn1write.h

Major activities within core team

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

- Mbed TLS 4.1/TF-PSA-Crypto 1.1 preparations
- PK module refactoring
- Prototyping and starting ML-DSA integration
- Bug bounty program
- Code size optimization initial investigation

Release Timeline

- 1.x/4.x
  - 1.0/4.0 (Oct 2025 – released): New major version
  - 1.1/4.1 (planned for end of March 2026): new LTS version
- 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