arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2026-01-12

Recent community activity (thank you!)

- tls#10557 frankencode - Fix: support empty PSK key hint in Client Key Exchange message
- tls#10558 frankencode - [3.6] Fix: support empty PSK key hint in Client Key Exchange message
- tls#10553 dc6jgk - allow negotiation of all use_srtp profile values currently listed by IANA
- tls#7159 daverodgman - pkcs7 - add support for signed attributes
- tls#10514 ng-gsmk - mbedtls_ssl_get_alert(): getter for fatal alerts
- tls#10372 dc6jgk - allow negotiation of all use_srtp profile values currently listed by IANA
- tls#10457 HaniAmmar - Add functions to export TLS traffic keys and sequence numbers for KTLS integration
- crypto#625 cxx194832 - SHA256 performance optimized by RVV

Recent community activity (thank you!)

Valerio @Nordic

- tls#10517 valeriosetti - Remove use of pk_debug()
- frame#257 valeriosetti - [framework] tests: pk: add a common function to create a PSA key out of predefined keys
- crypto#600 valeriosetti - [tf-psa-crypto] tests: pk: add a common function to create a PSA key out of predefined keys

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)

arm

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