arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath
2025-10-20

Recent community activity (thank you!)

- tls#10457 HaniAmmar - Add functions to export TLS traffic keys and sequence numbers for KTLS integration
- tls#10377 kraj - x509_crt: Zero-initialize mbedtls_x509_time at declaration
- merged: tls#10318 keith-packard - Avoid invalid gcc 14.3 warning about array bounds in mbedtls_xor
- tls#10431 rgqsch - Add challenge password to CSR Development
- tls#10432 rgqsch - Add challenge password to CSR mbedtls 3.6
- crypto#159 daverodgman - Neon impl of ChaCha20 (better size & perf)
- crypto#425 ilie-halip-nxp - scripts: driver_templates: fix few driver wrappers
- merged: crypto#391 keith-packard - Avoid invalid gcc 14.3 warning about array bounds in mbedtls_xor
- crypto#494 amjoul01 - Expand mbedtls_to_psa_error to LMS

Recent community activity (thank you!)

Valerio @Nordic

- tls#10447 valeriosetti - [3.6] psa: improve buffer size computation for static key slots
- frame#223 valeriosetti - tests: migrate tests using secp192[k|r]1 toward secp256[r|k]1 --> PK [1/2]
- crypto#492 valeriosetti - psa_load_builtin_key_into_slot: prevent accessing the PSA storage if key ID is in volatile range
- crypto#528 valeriosetti - [tf-psa-crypto] psa: improve buffer size computation for static key slots
- crypto#496 valeriosetti - PK: remove `pk_context::pk_ctx`
- crypto#460 valeriosetti - [tf-psa-crypto] Align header include guards with their new locations in TF PSA Crypto
- merged: crypto#477 valeriosetti - PK: remove RSA PKCS v2.1 unused code and fix tests
- crypto#513 valeriosetti - tests: migrate tests using secp192[k|r]1 toward secp256[r|k]1 --> PK [2/2]
- crypto#498 valeriosetti - PK: fix config dependencies and simplify guards
- crypto#497 valeriosetti - Remove the RSA key mutex

Major activities within core team

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

- Released Mbed TLS 4.0 and TF-PSA-Crypto 1.0
- Mbed TLS 4.0/TF-PSA-Crypto 1.0 bugfixes
- PK module refactoring
- Moving driver tests to Crypto CI
- Investigating ML-DSA integration

Release Timeline

- 1.x/4.x
  - 1.0/4.0 (Oct 2025 – released): New major version
  - 1.1/4.1 (TBD)
- 3.6 LTS supported until early 2027
  - 3.6.5 (Oct 2025 - released): Security fixes and bugfixes
  - 3.6.6 (TBD)

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה

ధన్యవాదములు