Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath & Gilles Peskine

2025-08-25

Recent community activity (thank you!)

- tls#10202 LoveKarlsson - [3.6] Fix alignment problems with IAR and Zephyr
- crypto#425 ilie-halip-nxp - scripts: driver_templates: fix few driver wrappers
- crypto#262 irwir - Add winsock2 header into build_info.h
- crypto#301 ilie-halip-nxp - scripts: driver_templates: call driver init/free
- crypto#410 LoveKarlsson - Made alignment typedefs more robust for IAR

Recent community activity (thank you!)

Valerio @Nordic

- merged: tls#10355 valeriosetti - tests: configuration-crypto: enable p192 curves in test_psa_crypto_without_heap
- tls#10356 valeriosetti - tests: configuration-crypto: enable p192 curves in test_psa_crypto_without_heap - SHADOW
- tls#10354 valeriosetti - [development] Remove 224-bit curves (3/5) - SHADOW
- merged: tls#10352 valeriosetti - [development] Remove 224-bit curves (3/5)
- merged: frame#200 valeriosetti - [framework] scripts: test_psa_compliance: add exceptions for tests using secp224r1 (4/6)
- frame#198 valeriosetti - [framework] Remove 224-bit curves (6/6)
- crypto#408 valeriosetti - [tf-psa-crypto] Remove 224-bit curves (5/6)
- crypto#394 valeriosetti - [tf-psa-crypto] Implement mbedtls_pk_can_do_psa (improved mbedtls_pk_can_do_ext) (1/2)

Major activities within core team

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

- TF-PSA-Crypto
  - First standalone components are now running in the CI
- Mbed TLS 4.0/TF-PSA-Crypto 1.0
  - Making low level crypto functions internal
  - Removing legacy types from public non-PSA interfaces
  - Removing legacy configuration options
  - PK API for 1.0
  - Released 4.0/1.0 beta for early evaluation

Release Timeline

- 1.0/4.0 code freeze planned for end of September 2025
- 3.6 LTS supported until early 2027
  - 3.6.1 (Aug 2024): mostly fixes related to TLS 1.3
  - 3.6.2 (Oct 2024): security fix
  - 3.6.3 (March 2024): supports a PSA key store in builds without malloc
  - 3.6.4 (June 2024): GCC 15 support, other bug and security fixes

arm

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