Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath, Gilles Peskine

2025-07-14

Recent community activity (thank you!)

- tls#10299 Mulling - mbedtls 2.28: Fix build and tests when building with gcc15
- tls#10202 LoveKarlsson - [3.6] Fix alignment problems with IAR and Zephyr
- tls#10270 Cube707 - add cast to fix IAR compiler warnings
- frame#155 Harshal5 - fix: Allow encrypt key usage for a CMAC operation
- crypto#249 Harshal5 - feat(drivers): Builtin CMAC driver use PSA cipher interface

Recent community activity (thank you!)

Valerio @Nordic

- crypto#308 valeriosetti - [tf-psa-crypto] PK: try storing all private RSA keys in PSA (3/3)

Major activities within core team

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

- Mbed TLS 4.0/TF-PSA-Crypto 1.0 APIs
  - Making low level crypto internal
  - Remove some obsolete crypto (DES, small curves)
  - PAKE moving to PSA Crypto 1.2 API (formerly was a beta API)
  - Lighter md.h and pk.h
  - Simplified RNG options
  - Miscellaneous small improvements
- Mbed TLS 4.0/TF-PSA-Crypto 1.0 products
  - Beta-testing the release process for split repositories
  - Fix some build/install script issues

Release Timeline

- 1.0/4.0 currently aiming for September 2025
  - Beta release early July
- 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 2025): supports a PSA key store in builds without malloc
  - **3.6.4 (1 July 2025): TLS-Exporter, 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