Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath, Gilles Peskine

2025-06-30

Recent community activity (thank you!)

- tls#10202 LoveKarlsson - [3.6] Fix alignment problems with IAR and Zephyr
- tls#10232 jean-baptisteboric-eaton - PKCS#7: add support for authenticated attributes and multiple certificates
- merged: tls#10200 aslze - [3.6] Fix build C++ apps with MSVC
- tls#10219 awesomekosm - Added shallow clone for submodules
- frame#176 jean-baptisteboric-eaton - Add additional PKCS#7 test artifacts
- merged: crypto#258 ccrugoPhilips - Fix MSVC build issue from MbedTls issue 7087
- crypto#320 jean-baptisteboric-eaton - Add OIDs for PKCS#7 authenticated attributes
- crypto#301 ilie-halip-nxp - scripts: driver_templates: call driver init/free

Recent community activity (thank you!)

Valerio @Nordic

- tls#10228 valeriosetti - [development] PK: try storing all private RSA keys in PSA (2/3) - Shadow
- merged: tls#10213 valeriosetti - [development] PK: try storing all private RSA keys in PSA (2/3)
- merged: tls#10237 valeriosetti - Remove temporary path fixes introduced in mbedtls#10225
- merged: tls#10240 valeriosetti - library: Makefile: use wildcard to select sources for crypto library
- tls#10227 valeriosetti - [development] Move Everest headers to a private subdirectory (1/2) - Shadow
- merged: tls#10225 valeriosetti - [development] Move Everest headers to a private subdirectory (1/2)
- merged: tls#10187 valeriosetti - [development] Always enable MBEDTLS_PK_USE_PSA_EC_DATA + use PSA interruptible operations as backend for PK restartable ones
- merged: frame#171 valeriosetti - [framework] PK: try storing all private RSA keys in PSA (1/3)
- crypto#308 valeriosetti - [tf-psa-crypto] PK: try storing all private RSA keys in PSA (3/3)
- merged: crypto#325 valeriosetti - Privatize content in Everest headers
- merged: crypto#319 valeriosetti - [tf-psa-crypto] Move Everest headers to a private subdirectory (2/2)

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
  - Removing legacy types from public interfaces
  - PAKE moving to PSA Crypto 1.2 API (formerly was a beta API)
  - Planning for further work in Q3: lighter md.h and pk.h, simplified RNG configuration, simplified error codes, …
- 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 (today 30 June 2025): TLS-Exporter, GCC 15 support, other bug and security fixes**

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