arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2025-06-02

© 2024 Arm

Recent community activity (thank you!)

- tls#9489 rsaxvc - Optimize software gcm_mult() routines on strictly-aligned systems
- merged: tls#10185 rojer - Mark TLS 1.2 algo suite definitons const
- merged: tls#8947 rojer - Mark ssl_tls12_preset_default_sig_algs const
- crypto#262 irwir - Add winsock2 header into build_info.h
- crypto#258 ccrugoPhilips - Fix MSVC build issue from MbedTls issue 7087
- crypto#152 LoveKarlsson - Fix IAR alignment issues if __packed has been redefined into a macro.

© 2024 Arm

Recent community activity (thank you!)

Valerio @Nordic

- tls#10192 valeriosetti - [development] Some pre-requisites for psa#299
- tls#10187 valeriosetti - [development] Always enable MBEDTLS_PK_USE_PSA_EC_DATA + use PSA interruptible operations as backend for PK restartable ones
- tls#10163 valeriosetti - [development] Always enable MBEDTLS_PK_USE_PSA_EC_DATA
- merged: tls#10190 valeriosetti - [development] Some prerequisites for PR #10187
- frame#154 valeriosetti - [framework] Add components-compiler.sh
- frame#166 valeriosetti - [framework] Always enable MBEDTLS_PK_USE_PSA_EC_DATA
- frame#167 valeriosetti - [framework] Remove MBEDTLS_USE_PSA_CRYPTO from PK module
- crypto#248 valeriosetti - [tf-psa-crypto] Add components-compiler.sh
- crypto#299 valeriosetti - [tf-psa-crypto] Always enable MBEDTLS_PK_USE_PSA_EC_DATA + use PSA interruptible operations as backend for PK restartable ones
- crypto#280 valeriosetti - [tf-psa-crypto] Always enable MBEDTLS_PK_USE_PSA_EC_DATA
- merged: crypto#278 valeriosetti - Remove mbedtls_pk_rsassa_pss_options
- merged: crypto#285 valeriosetti - [tf-psa-crypto] Remove MBEDTLS_USE_PSA_CRYPTO from PK module

© 2024 Arm

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
  - Last stages of MVP investigation
  - Making low level crypto functions internal
  - Removing legacy types from public non-PSA interfaces
  - Defining release process for split repositories

© 2024 Arm

Release Timeline

- 1.0/4.0 currently aiming for 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 (End of Q2 2024): TBD

© 2024 Arm

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

© 2024 Arm