Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2025-05-19

Recent community activity (thank you!)

- ttls#8947 rojer - Mark ssl_tls12_preset_default_sig_algs const
- tls#10169 tfloch - [Backport 3.6] adjust_legacy_from_psa: Add AES-XTS algorithm support
- tls#5819 polhenarejos - Add support for EdDSA with ed25519 curve (pure ed25519, ed25519ctx and ed25519ph)
- merged: docs#179 aaron-sierra - tutorial: Update URL for uIP TCP/IP stack
- crypto#262 irwir - Add winsock2 header into build_info.h
- crypto#287 tfloch - adjust_legacy_from_psa: Add AES-XTS algorithm support

Recent community activity (thank you!)

Valerio @Nordic

- merged: tls#10130 valeriosetti - [development] Restrict MBEDTLS_X509_RSASSA_PSS_SUPPORT
- merged: tls#10090 valeriosetti - [development] MBEDTLS_PLATFORM_GET_ENTROPY_ALT in 4.0
- tls#10163 valeriosetti - [development] Always enable MBEDTLS_PK_USE_PSA_EC_DATA
- frame#167 valeriosetti - [framework] Remove MBEDTLS_USE_PSA_CRYPTO from PK module
- frame#154 valeriosetti - [framework] Add components-compiler.sh
- frame#166 valeriosetti - [framework] Always enable MBEDTLS_PK_USE_PSA_EC_DATA
- crypto#285 valeriosetti - [tf-psa-crypto] Remove MBEDTLS_USE_PSA_CRYPTO from PK module
- crypto#278 valeriosetti - Remove mbedtls_pk_rsassa_pss_options
- crypto#248 valeriosetti - [tf-psa-crypto] Add components-compiler.sh
- merged: crypto#212 valeriosetti - [tf-psa-crypto] MBEDTLS_PLATFORM_GET_ENTROPY_ALT in 4.0
- crypto#280 valeriosetti - [tf-psa-crypto] Always enable MBEDTLS_PK_USE_PSA_EC_DATA
- merged: crypto#253 valeriosetti - [tf-psa-crypto] Restrict MBEDTLS_X509_RSASSA_PSS_SUPPORT

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

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

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה

ధన్యవాదములు