Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Gilles Peskine

2024-08-26

Recent community activity (thank you!)

Miscellaneous

- #8800 winterheart - Allow install headers to different location (mbedtls-3)
- merged: #9486 sergio-nsk - [Backport 3.6] Fix Mbed-TLS build when WIN32_LEAN_AND_MEAN macro is defined globally
- merged: #9485 sergio-nsk - Fix Mbed-TLS build when WIN32_LEAN_AND_MEAN macro is defined globally
- #9489 rsaxvc - Optimize software gcm_mult() routines on strictly-aligned systems
- #9218 casaroli - Make local functions and objects static
- #9423 BhanuPrakash-P - Fix pkcs8 unencrypted private key parsing with Attributes field

Recent community activity (thank you!)

Valerio Setti @Nordic

- #9448 valeriosetti - [Backport 3.6] PSA: use static key slots to store keys
- #9302 valeriosetti - PSA: use static key slots to store key

Major activities within core team

https://github.com/orgs/Mbed-TLS/projects/1

- Mbed TLS 3.6.1 (release expected this Friday)
  - Focus on regressions in 3.6.0
  - Mainly workarounds for TLS 1.3 issues: https://github.com/Mbed-TLS/mbedtls/issues/9223
- TF-PSA-Crypto — main focus in Q3
  - Splitting files, reworking some interfaces (configuration, platform, …)
  - https://github.com/Mbed-TLS/TF-PSA-Crypto
  - Will become upstream source for crypto in Mbed TLS
- Mbed TLS 4.0
  - https://github.com/orgs/Mbed-TLS/projects/15
  - PSA_CRYPTO_C / CLIENT always on
  - Consume TF-PSA-Crypto repository as source of PSA and crypto code
  - Remove some legacy interfaces & features
- Open for SPAKE2+ reviews (tasks defined on backlog board)

Release Timeline

- 3.6.1 expected Friday 30 August 2024
- 4.0 currently aiming for first half of 2025
- 3.6 LTS supported until early 2027
- 2.28 LTS ends supported life end of 2024

TF-PSA-Crypto 1.0 + Mbed TLS 4.0 highlights

- TLS 1.2: removing finite-field DH, static ECDH, PKCS#1v1.5 RSA encryption, CBC
- Crypto: removing PKCS#1v1.5 RSA encryption, DES, EC curves smaller than 250 bits
- Removing all crypto ALT (use PSA drivers instead)
- Removing low-level crypto APIs (use PSA APIs instead)
  - Removing cipher.h; Keeping parts of md.h and pk.h partially as transition layers
  - Removing direct access to bignum/ECC arithmetic
  - Removing direct access to DRBG

arm

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