Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2024-08-12

Recent community activity (thank you!)

Miscellaneous

- #9001 raymo200915 - Add PKCS#7 parser features for integrating MbedTLS with U-Boot
- #9423 BhanuPrakash-P - Fix pkcs8 unencrypted private key parsing with Attributes field
- merged: #8716 mschulz-at-hilscher - Use large GCM tables
- #9189 misch7 - Fix build of v3.6 (issues #9186 and #9188)
- #8354 mcagriaksoy - Add ignoring return value casting and Fix non-uniform cast
- #6294 jeremyherbert - Implement AES-GCM-SIV as per RFC 8452

Recent community activity (thank you!)

Valerio Setti @Nordic

- #9371 valeriosetti - psasim: use shared memory as messaging system for client-server communication
- merged: #9427 valeriosetti - psasim: small fixes to all.sh and test bash scripts
- #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

- 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
  - PSA_CRYPTO_C / CLIENT always on
  - Consume TF-PSA-Crypto repository as source of PSA and crypto code
  - Remove some legacy interfaces & features
- Mbed TLS 3.6.1
  - Focus on regressions in 3.6.0
  - Workarounds for TLS 1.3 issues: https://github.com/Mbed-TLS/mbedtls/issues/9210#issuecomment-2141498918
- Open for SPAKE2+ reviews (tasks defined on backlog board)

Release Timeline

- 3.6.1 end of 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

arm

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