Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath
2024-05-20

Recent community activity (thank you!)

- Valerio Setti @Nordic
  - #9121 - Add client-server build to all.sh
  - #9138 - Do not perform adjustments on legacy crypto from PSA, when MBEDTLS_PSA_CRYPTO_CLIENT && !MBEDTLS_PSA_CRYPTO_C

- Misc
  - #8113 AgathiyanB - Validate UTF-8 in DNs
  - #9082 andre-rosa - Add invalid padding_len check in get_pkcs_padding
  - #9132 andre-rosa - Backport 3.6: Add invalid padding_len check in get_pkcs_padding
  - #9139 bluerise - Silence gcc 12.2.0 warning
  - #8389 daantimmer - Use CMAKE_C_SIMULATE_ID when available to determine compiler
  - #8876 dannytsen - Adding PowerPC support using vector instructions for AES and GCM functions
  - #9123 eleuzi01 - Replace MBEDTLS_MD_CAN_MD5 with PSA_WANT_ALG_MD5
  - #9125 eleuzi01 - Replace MBEDTLS_MD_CAN_RIPEMD160 with PSA_WANT_ALG_RIPEMD160
  - #9119 jetm - docs: Add development branch section
  - #9105 jetm - ssl_client2: Add Host to HTTP GET request
  - #9118 jetm - ssl_client2: Add Host to HTTP GET request
  - #9127 nbfalcon - constant_time.h: add #ifdef __cplusplus guard
  - #9096 noahp - mbedtls_net_send API description typo fix
  - #8981 rojer - TLS handshake fragmentation support
  - #9155 ttytm - fix typo

Major activities within core team

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

- 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

- TF-PSA-Crypto
  - https://github.com/Mbed-TLS/TF-PSA-Crypto
  - Will become upstream source for crypto in Mbed TLS

Release Timeline

- 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

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה

ధన్యవాదములు