Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath
2024-06-03

Recent community activity (thank you!)

- Valerio Setti @Nordic
  - #9178 valeriosetti - adjust_legacy_crypto: enable CIPHER_C when PSA CMAC is builtin
  - merged: #8715 valeriosetti - Remove all internal functions from public headers
  - #9138 valeriosetti - Do not perform adjustments on legacy crypto from PSA, when MBEDTLS_PSA_CRYPTO_CLIENT && !MBEDTLS_PSA_CRYPTO_C
  - merged: #9121 valeriosetti - Add client-server build to all.sh

- Misc
  - merged: #9177 ttytm - Backport 3.6: fix typo
  - merged: #9155 ttytm - fix typo
  - #9183 MaJerle - Remove unnecessary casting for return value of mbedtls_calloc
  - #9189 misch7 - Fix build of v3.6 (issues #9186 and #9188)
  - #9119 jetm - docs: Add development branch section

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

4.0 Discussions

Please provide your feedback

- Consider removing support for the RSA key exchange in TLS 1.2 #8170
- Consider removing CBC cipher suites #9202
- Consider removing static ECDH cipher suites #9201
- Remove the dynamic SE interface in 4.0 #8151
- How to partially accelerate ECC #103
- Importing partial RSA private keys #105
- How to implement a custom ECC-based mechanism #102
- How to implement a custom RSA-based mechanism #104
- Consider removing DES #9164

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