arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2024-07-01

Recent community activity (thank you!)

Miscellaneous

- #9045 Troy-Butler - [Backport 3.6] Fix NULL argument handling in mbedtls_xxx_free() functions

- #8983 Troy-Butler - Fix NULL argument handling in mbedtls_xxx_free() functions

- #7977 ivq - Fix doc on GCM API

- merged: #8389 daantimmer - Use CMAKE_C_SIMULATE_ID when available to determine compiler

- #9294 juhaylinen - Disable allow_abbrev from Python scripts using argparse

- #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

- #9287 Wenxing-hou - Fix some typo for include folder

- #9295 juhaylinen - [Backport 3.6] Disable allow_abbrev from Python scripts using argparse

- #9296 juhaylinen - [Backport 2.28] Disable allow_abbrev from Python scripts using argparse

- #9285 mimok - Fix typo in platform_util.c

- merged: #7968 gowthamsk-arm - Use earliest latest compilers

- #8981 rojer - TLS handshake fragmentation support

arm

Recent community activity (thank you!)

Valerio Setti @Nordic

- #9237 valeriosetti - PSA client-server: support in the unit test framework

- #9302 valeriosetti - PSA: use static key slots to store keys

- merged: #9310 valeriosetti - psasim: complete support of PSA functions in psasim and add basic "smoke test" applications

- #9308 valeriosetti - psa: fix parameters' names of psa_key_derivation_verify_bytes()

- merged: #9305 valeriosetti - [Backport 3.6] Do not perform adjustments on legacy crypto from PSA, when MBEDTLS_PSA_CRYPTO_CLIENT && !MBEDTLS_PSA_CRYPTO_C

- merged: #9138 valeriosetti - Do not perform adjustments on legacy crypto from PSA, when MBEDTLS_PSA_CRYPTO_CLIENT && !MBEDTLS_PSA_CRYPTO_C

- merged: #9280 valeriosetti - psasim-server: add function to reset operations slots

- merged: #9278 valeriosetti - psa_sim: improve log prints

- merged: #9279 valeriosetti - psa_sim: make server ping time much faster

arm

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

- Mbed TLS 3.6.1
  - 3.6 might break some existing builds
  - Workarounds: https://github.com/Mbed-TLS/mbedtls/issues/9210#issuecomment-2141498918

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

arm

4.0 Discussions

Please provide your feedback

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

arm

4.0 Discussions

Please provide your feedback

- DRBG interfaces [#107](#107)

- Consider requiring *printf()* to support *size_t* printing [#9307](#9307)

- Requirements for the build system [#106](#106)

- Remove PKCS #1 encryption [#8459](#8459)

- Consider removing AESNI assembly [#8231](#8231)

arm

Release Timeline

- 3.6.1 coming soon

- 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

arm

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