Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2024-06-17

Recent community activity (thank you!)

- Valerio Setti @Nordic
  - #9138 valeriosetti - Do not perform adjustments on legacy crypto from PSA, when MBEDTLS_PSA_CRYPTO_CLIENT && !MBEDTLS_PSA_CRYPTO_C
  - #9237 valeriosetti - PSA client-server: support in the unit test framework
  - merged: #9219 valeriosetti - [Backport 3.6] adjust_legacy_crypto: enable CIPHER_C when PSA CMAC is builtin
  - merged: #9178 valeriosetti - adjust_legacy_crypto: enable CIPHER_C when PSA CMAC is builtin
  - merged: #9221 valeriosetti - [Backport 3.6] fix documentation of psa_hash_compare()
  - merged: #9220 valeriosetti - fix documentation of psa_hash_compare()
  - merged: #9222 valeriosetti - [Backport 2.28] fix documentation of psa_hash_compare()

- Misc
  - #9189 misch7 - Fix build of v3.6 (issues #9186 and #9188)
  - merged: #9241 lhuang04 - Set psk to NULL in ssl_psk_remove
  - merged: #9245 lhuang04 - Backport 3.6: Set psk to NULL in ssl_psk_remove
  - merged: #9246 lhuang04 - Backport 2.28: Set psk to NULL in ssl_psk_remove
  - #5824 polhenarejos - Add support to Ed448 in EdDSA
  - #5819 polhenarejos - Add support for EdDSA with ed25519 curve (pure ed25519, ed25519ctx and ed25519ph)
  - #6556 polhenarejos - XChaCha20 and XChaCha20-Poly1305 support.
  - #5823 polhenarejos - Add support for SHA-3 KMAC
  - #5822 polhenarejos - SHA-3 cSHAKE128 and cSHAKE256 support
  - #5821 polhenarejos - SHA-3 SHAKE128 and SHAKE256 support
  - #8236 silabs-Kusumit - PSA Key Derivation Verification APIs
  - #9218 casaroli - Make local functions and objects static

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

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

- 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

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה

ధన్యవాదములు