arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2024-07-29

Recent community activity (thank you!)

Miscellaneous

- #9423 BhanuPrakash-P - Fix pkcs8 unencrypted private key parsing with Attributes field
- #9421 mfil - Draft: Implement TLS-Exporter
- #9189 misch7 - Fix build of v3.6 (issues #9186 and #9188)
- #7762 chemandante - ECP self test enhanced to use all Weierstrass curves when NIST optimization is enabled
- #5824 polhenarejos - Add support to Ed448 in EdDSA
- #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
- #5819 polhenarejos - Add support for EdDSA with ed25519 curve (pure ed25519, ed25519ctx and ed25519ph)
- merged: #6866 mprse - Extracting SubjectKeyId and AuthorityKeyId in case of x509 V3 extensions v.2
- merged: #9285 mimok - Fix typo in platform_util.c
- merged: #9287 Wenxing-hou - Fix some typo for include folder
- #9127 nbfalcon - constant_time.h: add #ifdef __cplusplus guard

Recent community activity (thank you!)

Valerio Setti @Nordic

- #9371 valeriosetti - psasim: replace SystemV RPC as messaging solution
- #9400 valeriosetti - PSA client-server: test parity report
- merged: #9308 valeriosetti - psa: fix parameters' names of psa_key_derivation_verify_bytes()

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)

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

4.0 Discussions

Please provide your feedback

- DRBG interfaces #107
- Consider requiring *printf()* to support *size_t* printing #9307
- Requirements for the build system #106
- Remove PKCS #1 encryption #8459
- Consider removing AESNI assembly #8231

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
ધન્યવાદ
תודה
ధన్యవాదములు