Recent community activity (thank you!)

+ Valerio Setti @Nordic
  • merged: #8937 - Clarify the documentation of mbedtls_pk_setup_opaque
  • merged: #8987 - Test gap: mbedtls_pk_check_pair withMBEDTLS_PK_OPAQUE
  • merged: #9005 - [Backport 3.6] Clarify the documentation of mbedtls_pk_setup_opaque
  • merged: #9004 - [Backport 3.6] Test gap: mbedtls_pk_check_pair withMBEDTLS_PK_OPAQUE
  • #8986 - Improve test key generation in test_suite_pk

+ Misc
  • merged: #8874 stevenwdv - Fix compilation on macOS without apple-clang
  • merged: #8875 stevenwdv - [backport] Fix compilation on macOS without apple-clang
  • #8933 Biswa96 - pkg-config: fix static linking in Windows
  • #8983 Troy-Butler - Fix NULL argument handling in mbedtls_xxx_free() functions
  • #8645 casswarry0 - Using make with paramter GEN_FILES="" still requires Python
  • #6955 inorick - Guard ticket specific TLS 1.3 function with macro
  • #9001 raymo200915 - Add PKCS#7 parser features for integrating MbedTLS with U-Boot
  • #8945 rojer - mbedtls_debug_print_crt: Reduce stack usage
  • #8981 rojer - TLS handshake fragmentation support
  • #8946 rojer - Ignore MBEDTLS_ERR_SSL_PEER_CLOSE_NOTIFY when printing debug
  • #8950 rojer - Do not rely on undefined macro evaluating to 0
  • #8952 rojer - Streamline cleanup in MBEDTLS_X509.Safe_Snprintf
  • #8949 rojer - x509_crt: Add LWIP implementation of inet_pton
  • #8953 rojer - Remove unnecessary assignments
  • #8947 rojer - Mark ssl_tls12_preset_default_sig_algs const
  • #8236 silabs-Kusumit - PSA Key Derivation Verification APIs
  • #8907 szsam - Backport 2.28: ssl_mail_client: Fix unbounded write of sprintf()
  • #8897 szsam - ssl_mail_client: Fix unbounded write of sprintf()
**Major activities within core team**

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

- **Mbed TLS 3.6 LTS released** – support until early 2027
  - Accessor functions for fields made private in 3.0
  - TLS 1.3 early data, record size limit
  - Driver-only cipher & AEAD
  - Thread-safe PSA
  - PSA bridge – new APIs to help with transition from legacy to PSA

- **TF-PSA-Crypto**
  - [https://github.com/Mbed-TLS/TF-PSA-Crypto](https://github.com/Mbed-TLS/TF-PSA-Crypto)
  - Will become upstream source for crypto in Mbed TLS
  - Paused to focus on 3.6, resume in Q2

- **Planning Mbed TLS 4.0 – end 2024?**
  - PSA_CRYPTO_C / CLIENT always on
  - Consume TF-PSA-Crypto repository as source of PSA and crypto code
  - Remove some legacy interfaces & features

- **CI**
  - Testing on Arm coming soon
Release Timeline

3.6 LTS – early 2024 – support until early 2027
• TLS 1.3
  • Finish support for early data
  • Record size limit extension
  • Key export
• Driver-only cipher
• PSA thread safety
• Review private fields, add missing accessors
• Final 3.x release

Timeline
• 4.0 second half of 2024
• 2.28 LTS ends supported life end of 2024
Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Merci
감사합니다
ধন্যবাদ
شكرًا
धन्यवाद
हादीस
感谢