Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2025-04-07

Recent community activity (thank you!)

- tls#10100 frankencode - Added OID of Ed448 ECDSA signature algorithm
- tls#10112 etienne-lms - [Backport 3.6] Fix build warning related to deprecated DTLS connect ID
- tls#10113 etienne-lms - Fix build warning related to deprecated DTLS connect ID
- tls#8950 rojer - Do not rely on undefined macro evaluating to 0
- tls#8981 rojer - TLS handshake fragmentation support
- tls#10031 devinaberry - Create docker-image.yml
- tls#9421 mfil - Implement TLS-Exporter
- tls#10084 jurassicLizard - [Backport 3.6] add handling for default CMAKE_BUILD_TYPE values
- tls#10079 jurassicLizard - [development] introduce handling for default CMake Build types
- tls#10086 jurassicLizard - fix MBEDTLS_CONFIG_FILE not installing properly
- tls#8070 paul-elliott-arm - Backport 2.28: Convert code style checker script over to using git diff
- tls#8098 gowthamsk-arm - [Backport 2.28] Changes required for OpenSSL 3
- tls#8505 yuhaoth - Backports #8504: Add python version check
- tls#9296 juhaylinen - [Backport 2.28] Disable allow_abbrev from Python scripts using argparse
- tls#10080 DemiMarie - Disallow trailers in RSASSA-PSS algorithm identifiers
- crypto#240 frankencode - Added OID of Ed448 ECDSA signature algorithm
- crypto#190 Vge0rge - core: Update common.h to use GCC _Static_assert
- crypto#222 jurassicLizard - add handling for default CMAKE_BUILD_TYPE values
- crypto#217 DemiMarie - asn1parse: document behavior on unexpected tags
- crypto#216 DemiMarie - asn1parse: Require minimal-length encodings of lengths

Recent community activity (thank you!)

Valerio @Nordic

- merged: tls#10008 valeriosetti - [development] Add test_tf_psa_crypto_cmake_shared to components-build-system.sh
- tls#10090 valeriosetti - [development] MBEDTLS_PLATFORM_GET_ENTROPY_ALT in 4.0
- merged: tls#10032 valeriosetti - psasim: update README file
- merged: tls#10050 valeriosetti - [development] Remove the dynamic SE interface in 4.0
- frame#154 valeriosetti - [framework] Add components-compiler.sh
- merged: frame#141 valeriosetti - [framework] Add test_tf_psa_crypto_cmake_shared to components-build-system.sh
- merged: frame#151 valeriosetti - [framework] MBEDTLS_PLATFORM_GET_ENTROPY_ALT in 4.0
- merged: frame#147 valeriosetti - [framework] Remove the dynamic SE interface in 4.0
- crypto#212 valeriosetti - [tf-psa-crypto] MBEDTLS_PLATFORM_GET_ENTROPY_ALT in 4.0
- crypto#248 valeriosetti - [tf-psa-crypto] Add components-compiler.sh
- merged: crypto#181 valeriosetti - [tf-psa-crypto] Add test_tf_psa_crypto_cmake_shared to components-build-system.sh
- merged: crypto#197 valeriosetti - [tf-psa-crypto] Remove the dynamic SE interface in 4.0

Major activities within core team

https://github.com/orgs/Mbed-TLS/projects/18

- TF-PSA-Crypto
  - First standalone components are now running in the CI
- Mbed TLS 4.0/TF-PSA-Crypto 1.0
  - Focus is on re-planning and investigation
  - In parallel implementation tasks are being worked on
  - Removing RNG parameters from public facing functions
- Mbed TLS 3.6.3/2.28.10
  - Last release for the 2.28 LTS branch
  - MBEDTLS_PSA_STATIC_KEY_SLOTS feature in 3.6.3
  - Fix for the defragmentation bug preventing some TLS 1.3 connections

Release Timeline

- 1.0/4.0 currently aiming for September 2025
- 3.6 LTS supported until early 2027
  - 3.6.1 (Aug 2024): mostly fixes related to TLS 1.3
  - 3.6.2 (Oct 2024): security fix
  - 3.6.3 (March 2024): supports a PSA key store in builds without malloc
- 2.28 LTS has ended supported life

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה

ధన్యవాదములు