Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2025-03-24

Recent community activity (thank you!)

- tls#10084 jurassicLizard - add handling for default CMAKE_BUILD_TYPE values
- tls#10079 jurassicLizard - introduce handling for default CMake Build types
- tls#7693 DemiMarie - x509: Forbid empty extension lists
- tls#7688 DemiMarie - Rip out ancient Netscape cruft
- tls#10080 DemiMarie - Disallow trailers in RSASSA-PSS algorithm identifiers
- merged: tls#10051 Vge0rge - PSA core: Allow enabling one volatile/builtin key
- merged: tls#9096 noahp - mbedtls_net_send API description typo fix
- tls#10031 devinaberry - Create docker-image.yml
- tls#10036 tygyh - Update pylint to 2.7.0
- tls#9294 juhaylinen - Disable allow_abbrev from Python scripts using argparse
- tls#9295 juhaylinen - [Backport 3.6] Disable allow_abbrev from Python scripts using argparse
- tls#9994 tygyh - Update jinja2 to 3.1.6 for docs
- 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
- crypto#190 Vge0rge - core: Update common.h to use GCC _Static_assert
- merged: crypto#195 Vge0rge - core: Allow enabling one volatile/builtin key
- merged: crypto#193 hasheddan - Fix link to PSA Crypto API

Recent community activity (thank you!)

Valerio @Nordic

- tls#10008 valeriosetti - [development] Add test_tf_psa_crypto_cmake_shared to components-build-system.sh
- tls#10050 valeriosetti - [development] Remove the dynamic SE interface in 4.0
- merged: tls#9864 valeriosetti - [Backport 3.6] Move most of min_requirements.py to the framework
- merged: tls#9826 valeriosetti - [3.6] Move "easy" basic checks scripts to the framework
- merged: tls#9889 valeriosetti - [Backport 3.6] Move pkgconfig.sh to the framework
- merged: tls#9728 valeriosetti - [Backport 3.6] Revert & fix #9690 workarounds
- tls#10041 valeriosetti - [development] Make mbedtls_psa_register_se_key usable with opaque drivers
- merged: tls#10010 valeriosetti - [development] Add components to components-build-system.sh
- frame#141 valeriosetti - [framework] Add test_tf_psa_crypto_cmake_shared to components-build-system.sh
- frame#147 valeriosetti - [framework] Remove the dynamic SE interface in 4.0
- frame#151 valeriosetti - [framework] MBEDTLS_ENTROPY_HARDWARE_ALT in 4.0
- crypto#181 valeriosetti - [tf-psa-crypto] Add test_tf_psa_crypto_cmake_shared to components-build-system.sh
- crypto#197 valeriosetti - [tf-psa-crypto] Remove the dynamic SE interface in 4.0
- crypto#212 valeriosetti - [tf-psa-crypto] MBEDTLS_ENTROPY_HARDWARE_ALT in 4.0
- crypto#191 valeriosetti - [tf-psa-crypto] Make mbedtls_psa_register_se_key usable with opaque drivers
- merged: crypto#183 valeriosetti - [tf-psa-crypto] Add components to components-build-system.sh

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): will support a PSA key store in builds without malloc
- 2.28 LTS ends supported life after one last release in 25Q1

arm

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