arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2025-03-10

Recent community activity (thank you!)

- merged: tls#9872 rojer - Defragment incoming TLS handshake messages
- tls#10036 tygyh - Update pylint to 2.7.0
- tls#9998 tygyh - Add Jetbrains artifacts to .gitignore
- tls#10031 devinaberry - Create docker-image.yml
- merged: tls#10006 stgloorious - Rename BEFORE_COLON/BC to avoid conflicts
- crypto#190 Vge0rge - core: Update common.h to use GCC _Static_assert
- crypto#193 hasheddan - Fix link to PSA Crypto API
- crypto#189 amtkarm1 - Replace psa_pake_get_implicit_key() with psa_pake_get_shared_key()

Recent community activity (thank you!)

Valerio @Nordic

- tls#10010 valeriosetti - [development] Add components to components-build-system.sh
- tls#10041 valeriosetti - [development] Make mbedtls_psa_register_se_key usable with opaque drivers
- merged: tls#9972 valeriosetti - [development] Remove DHM module
- tls#10032 valeriosetti - psasim: update README file
- merged: tls#10027 valeriosetti - [development] md: allow dispatch to PSA whenever CRYPTO_CLIENT is enabled
- merged: tls#9562 valeriosetti - Backport 3.6: md: allow dispatch to PSA whenever CRYPTO_CLIENT is enabled
- tls#10008 valeriosetti - [development] Add test_tf_psa_crypto_cmake_shared to components-build-system.sh
- frame#145 valeriosetti - [framework] Make mbedtls_psa_register_se_key usable with opaque drivers
- merged: frame#140 valeriosetti - [Framework] md: allow dispatch to PSA whenever CRYPTO_CLIENT is enabled
- frame#141 valeriosetti - [framework] Add test_tf_psa_crypto_cmake_shared to components-build-system.sh
- crypto#183 valeriosetti - [tf-psa-crypto] Add components to components-build-system.sh
- crypto#191 valeriosetti - [tf-psa-crypto] Make mbedtls_psa_register_se_key usable with opaque drivers
- merged: crypto#175 valeriosetti - [tf-psa-crypto] Remove DHM module
- merged: crypto#188 valeriosetti - [tf-psa-crypto] md: allow dispatch to PSA whenever CRYPTO_CLIENT is enabled
- crypto#181 valeriosetti - [tf-psa-crypto] Add test_tf_psa_crypto_cmake_shared to components-build-system.sh

Major activities within core team

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

- TF-PSA-Crypto
  - https://github.com/Mbed-TLS/TF-PSA-Crypto
  - It is now the upstream source for crypto in Mbed TLS
  - The CI currently still pulls in Mbed TLS
  - Work is being done to remove this dependency
- Mbed TLS 4.0/TF-PSA-Crypto 1.0
  - PSA_CRYPTO_C / CLIENT always on
  - Consume TF-PSA-Crypto repository as source of PSA and crypto code
  - Remove some legacy interfaces & features
  - Focus is on re-planning and investigation
- 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

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

TF-PSA-Crypto 1.0 + Mbed TLS 4.0 highlights

- TLS 1.2: removing finite-field DH, static ECDH, PKCS#1v1.5 RSA encryption, ~~CBC~~
- Crypto: removing PKCS#1v1.5 RSA encryption, DES, EC curves smaller than 250 bits
- Removing all crypto ALT (use PSA drivers instead)
- Removing low-level crypto APIs (use PSA APIs instead)
  - Removing cipher.h; Keeping parts of md.h and pk.h partially as transition layers
  - Removing direct access to bignum/ECC arithmetic
  - Removing direct access to DRBG

arm

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