Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath
2025-01-27

Recent community activity (thank you!)

- tls#9894 BrianSipos - Add parsing of Name Constraints extension, allow handling raw Other Name
- tls#9421 mfil - Implement TLS-Exporter
- tls#9872 rojer - Defragment incoming TLS handshake messages
- tls#9701 daverodgman - Neon impl of ChaCha20 (better size & perf)
- tls#9797 NadavTasher - Added minimal TLSv1.3-only client configuration
- frame#122 benmcollins - data_files: Added two rsassa_pss keys (one pub, one priv) for test use
- frame#120 BrianSipos - Add test CA config with Name Constraints extension
- crypto#152 LoveKarlsson - Fix IAR alignment issues if __packed has been redefined into a macro.
- crypto#159 daverodgman - Neon impl of ChaCha20 (better size & perf)
- crypto#154 benmcollins - pk: Enable RSASSA-PSS key parsing
- crypto#147 BrianSipos - Register Name Constraints extension and BPv7 OIDs

Recent community activity (thank you!)

Valerio @Nordic

- tls#9910 valeriosetti - Remove DHE-PSK key exchange
- tls#9916 valeriosetti - Migrate DHE test cases to ECDHE
- tls#9562 valeriosetti - md: allow dispatch to PSA whenever CRYPTO_CLIENT is enabled
- tls#9917 valeriosetti - Remove the DHE-RSA key exchange
- merged: tls#9913 valeriosetti - Remove deprecated function mbedtls_x509write_crt_set_serial()
- merged: tls#9888 valeriosetti - Move pkgconfig.sh to the framework
- merged: tls#9889 valeriosetti - [Backport 3.6] Move pkgconfig.sh to the framework
- merged: tls#9864 valeriosetti - [Backport 3.6] Move most of min_requirements.py to the framework
- merged: tls#9863 valeriosetti - Move most of min_requirements.py to the framework
- frame#128 valeriosetti - [Framework] md: allow dispatch to PSA whenever CRYPTO_CLIENT is enabled
- frame#127 valeriosetti - [Framework] Remove the DHE-RSA key exchange
- merged: frame#116 valeriosetti - Move pkgconfig.sh to the framework
- merged: frame#105 valeriosetti - Move most of min_requirements.py to the framework
- crypto#165 valeriosetti - [TF-PSA-Crypto] Remove DHE-PSK key exchange
- crypto#158 valeriosetti - [TF-PSA-Crypto] Remove DHE-PSK key exchange
- merged: crypto#148 valeriosetti - [TF-PSA-Crypto] Move most of min_requirements.py to the framework

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 first half of 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

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