Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman

2024-01-15

Recent community activity (thank you!)

- Valerio Setti @Nordic
  - merged: #8649 - check_config.h not complete about builds without CIPHER_C
  - merged: #8641 - G3-G4 wrap-up
  - merged: #8632 - [G5] Make block_cipher work with PSA
  - merged: #7921 - TLS: Clean up ECDSA dependencies
  - #8681 - Conversion function between raw and DER ECDSA signatures
  - #8696 - Conversion function between raw and DER ECDSA signatures (alternative implementation)
  - #8664 - Conversion function from ecp group to PSA curve
  - #8666 - Export the mbedtls_md_psa_alg_from_type function
  - #8700 - psa_asymmetric_encrypt() doesn't work with opaque driver
- SiLabs
  - #8198 silabs-Kusumit - KDF incorrect initial capacity
- Hilscher
  - merged: #8695 jwinzig-at-hilscher - Backport 2.28: Fix bug in mbedtls_x509_set_extension
  - merged: #8688 jwinzig-at-hilscher - Fix bug in mbedtls_x509_set_extension
  - merged: #8511 mschulz-at-hilscher - Add benchmark for RSA 3072
  - merged: #8512 mschulz-at-hilscher - Alternative Timing compatible benchmark.c
  - merged: #8517 mschulz-at-hilscher - Fixes redundant declarations for psa_set_key_domain_parameters
  - #8510 mschulz-at-hilscher - Add LMS benchmark
- Misc
  - merged: #7455 KloolK - Comply with the received Record Size Limit extension
  - #7846 askourtis - ssl: fix critical extension handling regression
  - #8697 BensonLiou - Do not generate new random number while receiving HRR
  - #8413 dannytsen - Adding PowerPC (ppc64le) support using vector instructions for AES/GCM functions.
  - #6955 inorick - Guard ticket specific TLS 1.3 function with macro
  - #8665 ivq - Reduce many unnecessary static memory consumption
  - #8662 LocutusOfBorg - timing.c fix build failure with -O3 optimization level
  - #7604 zvolin - Add AES encrypted keys support for PKCS5 PBES2
- polhenarejos – EdDSA implementation
  - #5819 polhenarejos - Add support for EdDSA with ed25519 curve (pure ed25519, ed25519ctx and ed25519ph)
  - #5823 polhenarejos - Add support for SHA-3 KMAC
  - #5824 polhenarejos - Add support to Ed448 in EdDSA
  - #5822 polhenarejos - SHA-3 cSHAKE128 and cSHAKE256 support
  - #5821 polhenarejos - SHA-3 SHAKE128 and SHAKE256 support

arm

Major activities within core team

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

- 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
- TLS 1.3 early data, record size limit
  - In progress, continuing through Q1
- Driver-only cipher & AEAD
  - Largely complete, docs improvements in progress
- Thread-safe PSA
  - Design agreed, testing & implementation in progress
- Accessors for MBEDTLS_PRIVATE fields
  - Continue into Q1
- 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
- Planning Mbed TLS 3.6 LTS – Q1-Q2 2024
  - TLS 1.3 early data, record size limit
  - PSA multi-threading support
  - Accessor functions for fields made private in 3.0
  - Driver-only cipher and AEAD
  - Main focus for team in Q1