Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman

2023-11-06

Recent community activity (thank you!)

- Valerio Setti @Nordic
  - [G2] Create Cipher light
  - Add new symbol for PSA key enrollment functions
  - Make PEM use cipher.c when available
  - ~~Clean up curves handling in libtestdriver1 config~~
  - ~~Remove cipher/aead legacy dependencies from PSA test suites~~
  - ~~[G2] Make TLS work without Cipher~~
  - ~~Clarify driver handling of ALG_STREAM and ALG_ECB~~
  - ~~Fix error reporting in driver testing parity~~
  - ~~Improve location of MD_CAN macros~~
  - ~~Fix dependencies of mbedtls_pk_ec_ro and mbedtls_pk_ec_rw~~
  - ~~Add test component with all ciphers and AEADs accelerated only~~
  - ~~Change accel_aead component to full config~~
  - ~~PSA crypto should not depend on the cipher module~~
- SiLabs
  - PSA Key Derivation Verification APIs
  - KDF incorrect initial capacity
  - ~~PBKDF2 CMAC implementation~~
- Misc
  - Add AES encrypted keys support for PKCS5 PBES2 - zvolin
  - ~~Add accessors to config DN hints for cert request – gstrauss~~
  - Remove transparent key check in psa_asymmetric_encrypt/decrypto() - michael2012z
  - Update README.txt - SamayXD
  - Avoid warning with -Wsign-conversion - scaprile
  - Adding PowerPC (ppc64le) support using vector instructions for AES/GCM functions. - dannytsen
  - ~~AES-NI: use target attributes for x86 32-bit intrinsics - beni-sandu~~
  - Add CodeQL Workflow for Code Security Analysis - b4yuan
  - Use CMAKE_C_SIMULATE_ID when available to determine compiler - daantimmer
  - Fixes "CSR parsing with critical fields fails" - mschulz-at-hilscher
  - ~~Fix compiling AESNI in Mbed-TLS with clang on Windows - sergio-nsk~~
  - ~~Backport 2.28: Fix compiling AESNI in Mbed-TLS with clang on Windows - sergio-nsk~~
  - Remove trailing whitespace on grep command in prepare_release.sh - mcagriaksoy
  - Implement non-PSA pk_sign_ext() - tomi-font

arm

Major activities within core team

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

- Mbed TLS license change
  - Now Apache-2.0 OR GPL-2.0-or-later
  - 3.5.1, 2.28.6 coming this week under new license
  - Existing users can continue to use under Apache 2.0 license with no impact
- TF-PSA-Crypto
  - https://github.com/Mbed-TLS/TF-PSA-Crypto
  - Currently, read-only preview
  - Will become upstream source for crypto in Mbed TLS
- TLS 1.3 early data
- Driver-only cipher & AEAD
  - AES, GCM, CCM, ChachaPoly
- Thread-safe PSA
- Planning Mbed TLS 4.0 – H2 2024?
  - PSA_CRYPTO_C / CLIENT always on
  - Consume TF-PSA-Crypto repository as source of PSA and crypto code
  - Remove some legacy interfaces & features
- TF-PSA-Crypto – productization
- 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

arm