Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman

2023-09-25

Recent community activity (thank you!)

Valerio Setti @Nordic

- Make CTR-DRBG use cipher.c when available
- PSA crypto should not depend on the cipher module
- **driver-only ECC: curve acceleration macros**
- ~~driver-only ECC: Make PSA curves always a superset of ECP curves~~
- ~~Test with TF-M config and p256-m driver (part 1)~~
- ~~TLS: Clean up ECDSA dependencies~~
- ~~Test with ECC and FFDH accelerated and no bignum~~

Kusumit Ghoderao, Saketh Sunkishala @ Silicon Labs

- PSA Key Derivation Verification APIs
- PBKDF2: test output_key

EdDSA - Pol Henarejos

- Add support to Ed448 in EdDSA
- Add support for SHA-3 KMAC
- SHA-3 cSHAKE128 and cSHAKE256 support
- SHA-3 SHAKE128 and SHAKE256 support
- Add support for EdDSA with ed25519 curve (pure ed25519, ed25519ctx and ed25519ph)

Misc

- Fix MSVC error C4703 about possibly uninitialized variable in pkwrite.c – kouzhudong
- add missing requires documentation in mbedtls_config.h – jnmeurisse
- Fixes interface of version string functions - Mehmet Çağrı Aksoy @ Alten
- Fixes log level for got supported group message - Mehmet Çağrı Aksoy @ Alten
- Fix "inconsistent annotation" warnings - Mehmet Çağrı Aksoy @ Alten
- entropy: Implements getrandom's wrapper for NuttX – makejian
- Change type of parameter for mbedtls_cipher_info_from_values - Sweidan Omár
- Fix test suite SSL dependencies for DHE - Stephan Koch @ Oberon
- XChaCha20 and XChaCha20-Poly1305 support - Pol Henarejos

PKCS #7 – Beni Sandu

- pkcs7: add support for embedded certificates
- PKCS7: Add support for authenticated attributes

Major activities within core team

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

- Mbed TLS 3.5 - September – October 2023
  - Size optimization (including driver-only ECP, bignum)
  - p-256m – reduce code size for SECP256R1 ECDH and ECDSA
  - SHA-3
  - AES performance
  - PBKDF2 CMAC and HMAC
  - TLS 1.3 FFDH
  - TLS 1.3 server-side version negotiation

- Planning Mbed TLS 4.0 – mid 2024?
  - PSA_CRYPTO_C / CLIENT always on
  - Consume PSA-Crypto repository as source of PSA and crypto code
  - Remove some legacy interfaces & features

- PSA Crypto – prototyping move to separate repository

- CI
  - Testing on Arm coming soon

- Planning Mbed TLS 3.6 LTS - end of 2023 (maybe early 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

Release Plans

- **3.5 – late September or early October**
  - Size optimization (including driver-only ECP, bignum)
  - p-256m – reduce code size for SECP256R1 ECDH and ECDSA
  - SHA-3
  - AES performance
  - PBKDF2 CMAC and HMAC
  - TLS 1.3 FFDH
  - TLS 1.3 server-side version negotiation

- **3.6 LTS – end of 2023 or early 2024**
  - TLS 1.3
    - Finish support for early data
    - Record size limit extension
    - Key export
  - Driver-only cipher
  - PSA thread safety
  - Review private fields, add missing accessors
  - Final 3.x release

- **Timeline**
  - 3.5 end of September / early October
  - 3.6 LTS end of 2023 or early 2024
  - 4.0 second half of 2024