Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman
2024-01-29

Recent community activity (thank you!)

Valerio Setti @Nordic

- merged: #8664 - Conversion function from ecp group to PSA curve
- merged: #8666 - Export the mbedtls_md_psa_alg_from_type function
- merged: #8700 - psa_asymmetric_encrypt() doesn't work with opaque driver
- #8734 - Add test for driver-only HMAC
- #8703 - Conversion function between raw and DER ECDSA signatures (guards in ASN1)
- #8740 - Move RSA basic key parsing/writing to rsa.c
- #8717 - PSA FFDH: feature macros for parameters
- #8715 - Remove all internal functions from public headers

SiLabs

- #8198 silabs-Kusumit - KDF incorrect initial capacity

Hilscher

- #8510 mschulz-at-hilscher - Add LMS benchmark
- #8716 mschulz-at-hilscher - Use large GCM tables

Misc

- merged: #8662 LocutusOfBorg - timing.c fix build failure with -O3 optimization level
- merged: #8751 trofi - tests: fix calloc() argument list (gcc-14 fix)
- merged: #8726 v1gnesh - Update entropy_poll.c to allow build in z/OS
- #8697 BensonLiou - Do not generate new random number while receiving HRR
- #8733 ivq - Add back restriction on AD length of GCM
- #8757 merryhime - CMake: Only use Apple-specific ranlib flags with Apple-provided toolchains
- #8754 Redfoxymoon - fix build for midipix
- #7604 zvolin - Add AES encrypted keys support for PKCS5 PBES2

Arm

- #8729 adeaarm - Add a client view of the multipart contexts
- #8745 adeaarm - Put the id field at the end of the psa_key_attributes_s structure
- #8691 billatarm - pkg-config: add initial pkg-config files

Major activities within core team

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

- Minor release: 3.5.2 and 2.28.7
  - Fix timing side-channel in RSA
  - Fix buffer-overflow in X.509
- Mbed TLS 3.6 LTS in progress – support until early 2027
  - Accessor functions for fields made private in 3.0
  - TLS 1.3 early data, record size limit
  - Driver-only cipher & AEAD
  - Thread-safe PSA
  - PSA bridge – new APIs to help with transition from legacy to PSA
- 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

- 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

Release Timeline

- **3.5 – October 5**
  - 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

- **3.5.2 – 2024-01-26**
  - Same as 3.5.1, but with two security bug fixes

- **3.6 LTS – early 2024 – support until early 2027**
  - 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 early 2024
  - 4.0 second half of 2024
  - 2.28 LTS ends supported life end of 2024