Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman

2024-02-26

Recent community activity (thank you!)

- Valerio Setti @Nordic
  - merged: #8734 - Add test for driver-only HMAC
  - merged: #8804 - mbedtls_rsa_parse_key and mbedtls_rsa_parse_pubkey accept trailing garbage
  - merged: #8826 - RSA keys set to PSS/OAEP padding perform PKCS1v1.5 when MBEDTLS_USE_PSA_CRYPTO is enabled
  - #8842 - Generalize mbedtls_pk_setup_opaque to MBEDTLS_PSA_CRYPTO_CLIENT
  - #8774 - Implement mbedtls_pk_copy_from_psa
- Hilscher
  - merged: #8716 mschulz-at-hilscher - Use large GCM tables
- Misc
  - merged: #8661 BensonLiou - use mbedtls_ssl_session_init() to init session variable
  - merged: #8841 BensonLiou - use mbedtls_ssl_session_init() to init session variable
  - merged: #8660 ivq - Fix a comment in ecp
  - merged: #8818 PiotrBzdrega - Backport 2.28: move entropy init prior arguments number recognition
  - merged: #8810 PiotrBzdrega - move entropy init prior arguments number recognition
  - #8697 BensonLiou - Do not generate new random number while receiving HRR
  - #8413 dannytsen - Adding PowerPC (ppc64le) support using vector instructions for AES/GCM functions.

Major activities within core team

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

- 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

arm