Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman
2022-07-04

Recent community activity (thank you!)

- Glenn Strauss
  - Two X.509 code-size and memory-size PRs
  - Merged DN hints accessor for cert request
  - Merged PR inlining mbedtls_x509_dn_get_next
- EdDSA
  - Community contribution of SHA-3, SHAKE, CSHAKE, KMAC Ed25519 and Ed448 (legacy interface)
  - Started review of SHA-3 (legacy interface)
  - Other items will aim to progress as a background task during 2022
  - Merged bugfix for Curve448 order
- Misc
  - make dependency tidy-up
  - cmake improvement for IAR warnings

- François Beerten / Silex
  - PSA driver support for entropy gathering #5437
    - Design review complete
  - Updated following feedback – ready for more review?
- Archana Madhavan / SiLabs
  - PR for code-gen 1.1 (introduction of JSON driver tooling) #5396
  - Going through cycle of review & updates, progressing towards resolution
- SecureMark-TLS / Cuno Pfister
  - PR opened to add support for Mbed TLS 3.1

Major activities within core team

- Mbed TLS 3.2 – aiming for July 11
  - Working on merging last few items
  - Aim to address most 3.0 API issues reported by community

- Website offline
  - tls.mbed.org went down
  - Pointed at the new website, but old content is missing
  - We are working to restore most of the content very soon

- OpenCI
  - Running well, expect to fully transition to this soon
  - Windows coming very soon – currently FreeBSD / Ubuntu
  - Please let us know your feedback

- TLS 1.3
  - Migrating to using PSA – almost complete
  - Server side functionality complete
  - PSK started
    - Community help welcomed on these!

- Storage format stabilization complete
  - Testing & documentation to assure stable format for non-volatile storage

- PSA Crypto
  - On-going collaboration including Arm, SiLabs, Nordic
  - Use of accelerators for (almost) all crypto in X.509, TLS complete
  - Isolation of long-term secrets (e.g. PSK, private keys) almost complete
  - Planning Q3 work
    - Focus on code size via PSA_CRYPTO_CONFIG
    - Restartable signing API
    - PSA 1.1; misc. gaps; EC J-PAKE implementation

- Review workload
  - Struggling for review bandwidth – any assistance from the community is hugely valuable
  - Easing the general review load accelerates progress on work prioritized by the community