arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman

2022-08-15

Recent community activity (thank you!)

- PSA size optimisation
  - Support hashes via driver (with no software implementation) in EC J-PAKE
- Misc
  - Coverity fixes
  - Support SNI without X.509
  - Windows CMAKE improvement
  - Bugfix to mbedtls_ctr_drbg_free with AES_ALT enabled
  - Callback for handling CRL critical extensions
- QUIC
  - Request for info on roadmap
  - MPS needs to be done first; so not in 2022

- François Beerten / Silex
  - PSA driver support for entropy gathering #5437
    - Design review complete
    - Francois working on testing (currently paused)
- Archana Madhavan / SiLabs
  - PR for code-gen 1.1 (introduction of JSON driver tooling) #5396
  - Going through cycle of review & updates, progressing towards resolution
- EdDSA
  - Community contribution of SHA-3, SHAKE, CSHAKE, KMAC Ed25519 and Ed448 (legacy interface)
  - Review steadily progressing through 2022
  - Community interest in merging this (e.g. #6166)

arm

Major activities within core team

- Quiet period – many people on holiday :-)

- Mostly focused on Q3 plans
  - PSA code-size optimisations
  - Bignum performance optimization
  - TLS 1.3 PSK
  - PKCS #7

- Website
  - tls.mbed.org went down
  - Pointed at the new website, but some old content is missing
  - Currently restoring old content via ReadTheDocs

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

- 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