Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman
2022-12-05

Recent community activity (thank you!)

- EC J-PAKE – Nordic
  - Support for opaque keys via PSA EC J-PAKE in TLS
  - Test improvements
  - Use via PSA in TLS 1.2

- PKCS #7 parsing - IBM
  - First draft merged
  - Further improvements & testing needed

- LMS (LMS_SHA256_M24_H20)
  - Allocate memory for larger trees on the heap

- Misc
  - CMake – move .cmake files to standard location

- 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)

Major activities within core team

- Mbed TLS 3.3 – on track for December 14
  - List of user-visible changes
    - https://github.com/Mbed-TLS/mbedtls/tree/development/ChangeLog.d
- Code style
  - A more standardized code style is coming – see #6591
- PSA code-size optimisations
  - (remove sw implementation when hw driver present)
  - Re-planning to address architectural issues
- Bignum performance optimization
  - Lots of activity on new interface
- TLS 1.3
  - Early data in progress
- PKCS #7 review
  - First draft of parser merged – not yet production-ready
  - Improvements on-going
- Interruptible sign/verify hash
  - Implementation started, planned for Q4

- Website
  - New website is up – most content restored
  - Includes knowledge-base and security advisories
  - Community contributions welcome via GitHub
- CI
  - Reduced testing load – internal CI healthy
  - OpenCI functional, but experimenting to get best perf
  - 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