arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman

2022-11-21

Recent community activity (thank you!)

- EC J-PAKE - Nordic
  - Test improvements
  - Support for PSA EC J-PAKE in TLS 1.2
  - Driver dispatch implementation review
- PKCS #7 parsing - IBM
  - Close to approval – but some dependency issues emerged
- Driver wrapper code generation - SiLabs
  - Latest updates look good
- LMS
  - Add support for LMS_SHA256_M24_H20
- XchaCha20 and XChaCha20-Poly1305 support
- Misc
  - Cmake tidy-up
  - Error handling in example program dh_genprime
  - TLS debug message fix
  - Improvement to secp256r1 internal representation
  - Test for mbedtls_x509write_csr_set_extension()
  - Improve x509_info_subject_alt_name() formatting
  - TLS and X.509 small optimisations
  - Fix memory leak in ecp_mul_comb()
- Misc bignum optimisations – Glenn Strauss
  - Closed as we are reworking bignum
- 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

- Mbed TLS 3.3 - December 14
  - Finishing up tasks before code-freeze (Nov 30)
- Code style
  - A more standardized code style is coming – see #6591
- PSA code-size optimisations
  - (remove sw implementation when hw driver present)
  - Completed work on hashes, removing MD dependency
  - Re-planning to address architectural issues
- Bignum performance optimization
  - Lots of activity on new interface
- TLS 1.3
  - Early data started
- PKCS #7 review
  - Parsing first, then generation
- 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 much slower, experimenting
  - 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