arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman
2022-09-26

Recent community activity (thank you!)

- Support compressed ECP points – Glenn Strauss
  - Useful for interop testing, WPA client, openwrt
- EC J-PAKE - Nordic
  - Use PSA for EC J-PAKE in TLS 1.2 in review
  - Driver dispatch in review
  - PSA support merged
  - 36 PRs from Neil Armstrong – thanks!
- PKCS #7 parsing - IBM
  - Updating following round of review
- AES-GCM-SIV – Jeremy Herbert
  - Will need to block out time for review
- Misc
  - X.509 subject alt name – encoding fix
  - Windows file copy fix
  - Support SNI without X.509 (for DTLS & PSK)
- 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

- PSA code-size optimisations
  - (remove sw implementation when hw driver present)
  - Completed work on hashes, removing MD dependency
  - Planned Q4 – cipher and AEAD
- Bignum performance optimization
  - Design complete, initial PRs under way
- TLS 1.3
  - PSK looks on-track for Q3 completion
  - Early data breakdown for Q4 in progress
- PKCS #7 review
  - Parsing first, then generation
- LMS
  - Iterating through review process
- Interruptible sign/verify hash
  - Design in review, planned for Q4

- Website
  - New website is up – most content restored
  - Includes knowledge-base and security advisories
  - Community contributions welcome via GitHub
- OpenCI
  - Running well, expect to fully transition to this soon
  - Now running against all platforms with good performance
  - 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