arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman
2022-11-07

Recent community activity (thank you!)

- EC J-PAKE - Nordic
  - Use PSA for EC J-PAKE in TLS 1.2 in rework
  - Driver dispatch – needs rework

- PKCS #7 parsing - IBM
  - Close to approval – but some dependency issues emerged

- Driver wrapper code generation - SiLabs
  - Latest updates look good

- Misc
  - Fix (non-security) timing leak in ecp_mul_mxz()
  - Unit test for mbedtls_x509write_csr_set_extension()
  - Compile fix for Centos 7 aarch64

- Misc X.509 – Glenn Strauss
  - 4 x performance & memory improvement
  - Support SAN IP address in hostname verification

- 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
  - 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
  - Design in review, planned for Q4
- Mbed TLS 3.3
  - Working towards release in December

- Website
  - New website is up – most content restored
  - Includes knowledge-base and security advisories
  - Community contributions welcome via GitHub
- CI
  - Lots of performance issues over last few weeks
  - Overloaded CI a major part of this – reducing test load
  - OpenCI much slower, investigating
  - 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