Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman
2023-03-13

Recent community activity (thank you!)

- Driver-only – Valerio Setti @ Nordic
  - Various PRs & review to enable compiling out software implementation when a driver is present
- Windows threading using srwlock – fwc-dc
- Support 8-byte nonce in ChaCha20 - Kusumit Ghoderao @ Silicon Labs
- Read and write X25519 and X448 keys in RFC8410 format - Jethrogb & Gijs Kwakkel
- ASN.1 parsing robustness improvements x 4 – Demi Marie Obenour @Invisible Things Lab
- PSA misc bug fixes x 2 – Joakim Andersson @ Nordic
- Compile fixes x 4 – Sergey Nsk
- PSA test fixes – Stephan Koch @ Oberon

Major activities within core team

- Working towards Mbed TLS 3.4 at end of March
  - PKCS #7
  - PSA interruptible sign/verify
  - EC J-PAKE improvements
- Misc. OPC-UA PRs – various X.509 parsing & cert/CSR generation updates
- PSA Crypto – prototyping move to separate repository
- PKCS #7 review
  - Several improvements merged, support for detached signatures almost complete
  - Various additional features could be planned for future
- Interruptible sign/verify hash
  - Now complete
- EC J-PAKE driver dispatch
- Driver-only hashes – in progress
- Historical review – items older than one year
  - Currently working through some old issues
- CI
  - OpenCI functional
  - Working on performance improvements
- 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

arm