# Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman

2023-02-27

# Recent community activity (thank you!)

- Driver-only – Valerio Setti @Nordic
  - ECC dependency fix
  - ECDSA: enable ECDSA-based TLS 1.2 key exchanges
  - Some MAX_SIZE macros are too small when PSA ECC is accelerated
- EdDSA – Pol Henarejos
  - Add support to Ed448 in EdDSA
  - Add support for SHA-3 KMAC
- Support 8-byte nonce in Chacha20 – Silicon Labs
- asn1parse – docs / tidy-up – Demi Marie @Invisible Things Lab
- PKCS 7 fixes – Demi Marie
- PKCS 7 support for internal certificates; signed attributes - Joakim Sindholt
- Misc
  - Compile fix in psa_key_derivation_abort - Nordic
  - Test improvement for Edwards curves - Oberon
  - Test improvement for psa_asymmetric_encrypt - Oberon
  - Fix unreachable code compiler warning - sergio-nsk
  - Docs improvement for Short Weierstrass curves – Chien Wong @IVQ
  - Improve formatting of debug messages – valord577
  - Discussion on threading support in Windows using SRW locks – Sergey Seroshtan

# Major activities within core team

- Working towards Mbed TLS 3.4 in March
- Code style
  - More standard code-style deployed, enforced by CI
  - Use mbedtls-rewrite-branch-style from mbedtls-docs to update in-flight PRs
- 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
  - PRs for new features shared from community
- Interruptible sign/verify hash
  - Implementation merged, test improvements following
- EC J-PAKE driver dispatch
- Driver-only hashes – in progress
- Historical review – items older than one year
  - Currently working through some old issues
- 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

# PSA Header collisions

- Problem: client-server projects like TF-M have issues with include header collisions
  - Issues with crypto_platform.h and crypto_struct.h
  - https://github.com/orgs/Mbed-TLS/projects/1#column-19369178
- Currently engaging with TF-M to resolve
  - Solution looks quite simple – see above link
  - Please comment on the GitHub issues if you have an interest in this topic
- Looks like it may be a simple fix
  - If this turns out to be the case, we will target Mbed TLS 3.4