Mbed TLS Tech Forum

Dave Rodgman
2022-03-14

Community activity (thank you!)

- Neil Armstrong / Nordic
  - Lots of PRs submitted for Use PSA Crypto More epic – 4 merged, 7 in review
  - Several reviews
- Archana Madhavan / SiLabs
  - PR for code-gen 1.1 (introduction of JSON driver tooling)
    - Updated, awaiting further review
- Mikhail Labiuk / OMP
  - Reviewing PSA thread safety requirements
- Steven Cooreman / SiLabs
  - Zeroization improvement; PSA dependency cleanup - merged
- Peter Spacek / SiLabs
  - Use PSA for hashing in X.509 and TLS - merged
- François Beerten / Silex
  - PSA driver support for entropy gathering – in review
- Various (lighttpd, IoTerop, …)
  - Accessors for various fields made private in Mbed TLS 3.0 – issues, discussions & PRs

Mbed TLS major activities within core team

- OpenCI
  - Some parts of CI now publicly visible – more coming
- GitHub migration from ArmMbed to Mbed-TLS organization in progress
  - Better reflect independence from Mbed OS projects / TF.org ownership
  - Easier management of GitHub (e.g., team members, etc)
- TLS 1.3
  - Client side progress: version negotiation, Certificate Verify message
  - Will start server side functionality and PSK in Q2
- 3.0 follow-up
  - Working on adding accessor functions for some things dropped from the public API in 3.0
  - Aim to cover most/all issues reported by community for Mbed TLS 3.2

- Storage format stabilization
  - Testing & documentation to assure stable format for non-volatile storage
- PSA Crypto
  - On-going collaboration including Arm, SiLabs, Nordic
- SHA-256 and SHA-512 performance
  - Optimisations for aarch64 crypto extensions –
    SHA-256 around 7x perf uplift (merged)
    SHA-512 in progress
- 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