Community PR activity (thank you!)

- Neil Armstrong / Nordic
  - Lots of PRs submitted for Use PSA Crypto
  - More epic
  - Most awaiting review

- Archana Madhavan / SiLabs
  - Submitted PR for code-gen 1.1 (introduction of JSON driver tooling)
  - #5067 seems obsoleted by #5137 – should we close this?

- Mikhail Labiuk / OMP
  - Reviewing PSA thread safety requirements

- Steven Cooreman / SiLabs
  - Zeroization improvement; PSA dependency cleanup

- Peter Spacek / SiLabs
  - Use PSA for hashing in X.509 and TLS

- febdoctor / Silex (?)
  - PSA driver support for entropy gathering – in review
Mbed TLS major activities within core team

• OpenCI
  • Expect to have some publicly visible CI results visible in March

• 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
  • Server side paused until Q2

• 3.0 follow-up
  • Working on adding accessor functions for some things dropped from the public API in 3.0

• Storage format stabilization
  • Testing & documentation to assure stable format for non-volatile storage

• PSA Crypto
  • On-going collaboration including Arm, SiLabs, Nordic

• 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