Recent community activity (thank you!)

- SecureMark-TLS / Cuno Pfister
  - [PR opened](#) to add support for Mbed TLS

- Neil Armstrong / Nordic
  - Several PRs on EC J-PAKE PSA support

- EdDSA
  - Community contribution of SHA-3, SHAKE, CSHAKE, KMAC Ed25519 and Ed448 (legacy interface)
  - Started review of SHA-3 (legacy interface)
  - Other items will aim to progress as a background task during 2022
  - Collaboration on adding tests to Curve448 bugfix

- Peter Spacek / SiLabs
  - Use PSA for hashing in TLS 1.3 – #5727 merged

- François Beerten / Silex
  - PSA driver support for entropy gathering #5437
    - Design review complete
  - Updated following feedback – ready for more review?

- Archana Madhavan / SiLabs
  - PR for code-gen 1.1 (introduction of JSON driver tooling) #5396
  - Going through cycle of review & updates, progressing towards resolution

- Misc
  - IAR build improvement
Major activities within core team

• Mbed TLS 3.2 – aiming for end of Q2
  • 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
  • May slip to July

• Website offline
  • tls.mbed.org is down – we are working to restore this very soon

• OpenCI
  • Running well, expect to fully transition to this soon
  • Windows coming very soon – currently FreeBSD / Ubuntu
  • Please let us know your feedback

• TLS 1.3
  • Migrating to using PSA – almost complete
  • Server side functionality mostly complete
  • PSK started
    – Community help welcomed on these!

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

• PSA Crypto
  • On-going collaboration including Arm, SiLabs, Nordic
  • Use of accelerators for (almost) all crypto in X.509, TLS complete
  • Isolation of long-term secrets (e.g. PSK, private keys) almost complete
  • Planning Q3 work – PSA 1.1; misc. gaps; code size (via PSA_CRYPTO_CONFIG)

• 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