arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman

2022-06-06

Recent community activity (thank you!)

- 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
- Peter Spacek / SiLabs
  - Use PSA for hashing in TLS 1.3 – #5727 very near completion
- François Beerten / Silex
  - PSA driver support for entropy gathering #5437
    - Design review complete
  - Waiting for updates re. code review & alignment on tests – in recent development
- 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
  - Coverity fix merged (Leo Rosen)
  - Support for cmake FetchContent merged (Robert Shade)

Major activities within core team

- OpenCI
  - Working on improving performance – now looking much better
  - 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!
- 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
- 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 almost complete
  - Isolation of long-term secrets (e.g. PSK, private keys) almost complete
  - Support for PSA 1.1 planned
- Performance
  - Bignum and ECP optimization started
- 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