arm

Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Dave Rodgman
2023-01-16

Recent community activity (thank you!)

- Read & write RFC8410 keys – Fortanix
  - Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure

- X.509 size & perf improvements – Glenn Strauss
  - x509_info
  - mbedtls_x509_time

- Support callbacks for parsing CRL critical extensions - Grégory Pinel

- X.509 hostname verification – support IPAddress subject alternate names – Glenn Strauss

- Misc
  - IAR warning fixes
  - X.509 serial handling fix

Major activities within core team

- Mbed TLS 3.3 – released December 14
  - Also released Mbed TLS 2.28.2 LTS
  - Available on the releases page
  - Features include
    - DTLS connection ID (support RFC 9146)
    - LMS signature verification (LMS_SHA256_M32_H10)
    - PSA support for EC J-PAKE
    - Support for TLS 1.3 pre-shared keys & session-resumption

- 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
  - Improvements on-going

- Interruptible sign/verify hash
  - Implementation started, planned for early Q1

- EC J-PAKE driver dispatch

- 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