

The background features a dark blue, futuristic aesthetic with a central image of a smartphone. The phone's screen displays a grid of binary code (0s and 1s). A glowing cyan line, resembling a laser or data stream, originates from the top left and points towards the phone. To the right of the phone, a glowing cyan fingerprint is visible. The overall scene is filled with abstract digital patterns, including lines and small 'x' marks, suggesting a high-tech or cybersecurity environment.

arm

Mbed TLS Tech Forum

<https://github.com/Mbed-TLS>

Janos Follath

2026-06-15

Recent community activity (thank you!)

- + tls#10731 AmyChan-Intel - library/alignment.h: Fix 'MBEDTLS_GCC_VERSION' is not defined error
- + tls#10767 eyupcanakman - Fix mbedtls_x509_dn_gets buffer too small for long DN values
- + tls#10616 nandojve - x509: Parse all certificate policy OIDs per RFC 5280
- + frame#308 sigvartmh - Add Spake2p support to test framework
- + frame#307 asmillby - scripts: Add dispatch include path and new generation location
- + crypto#801 AmyChan-Intel - 1.1: core/alignment.h: Fix 'MBEDTLS_GCC_VERSION' is not defined error
- + crypto#800 AmyChan-Intel - core/alignment.h: Fix 'MBEDTLS_GCC_VERSION' is not defined error
- + crypto#810 sigvartmh - SPAKE2+ PSA PAKE API support
- + crypto#809 asmillby - Complete the move of driver wrappers to the dispatch/ directory
- + crypto#806 bpcyril-jpg - Revert "include tf_psa_crypto_platform_requirements.h in tf_psa_crypto_config.c"
- + crypto#798 ChakshuGupta13 - fix: zeroize stack buffer containing private key in deterministic ECDSA
- + crypto#797 ChakshuGupta13 - fix: zeroize stack buffer containing private key in deterministic ECDSA

Major activities within core team

<https://github.com/orgs/Mbed-TLS/projects/18>

- + ML-DSA integration
 - Priority to bootloader/firmware use cases
- + Bug bounty program
- + Mbed TLS 4.2/TF-PSA-Crypto 1.2 preparations
 - Minor improvements for driver integration

Release Timeline

- + 1.x/4.x development
- + 1.1.x/4.1.x LTS supported until March 2029
 - 1.1.0/4.1.0 released on 2026-03-31
- + 3.6 LTS supported until early 2027
 - 3.6.6 (2026-03-31): Security fixes and bugfixes

arm

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה

ధన్యవాదములు