

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, suggesting biometric security. The overall scene is filled with faint, glowing lines and dots, creating a sense of digital connectivity and data flow.

arm

Mbed TLS Tech Forum

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

Janos Follath, Gilles Peskine
[2026-05-18](#)

Recent community activity (thank you!)

- + [tls#10715](#) Nadav0077 - Harden TLS 1.3 serialized session loading
- + [tls#10752](#) erorndev - ssl: reject trailing bytes in TLS 1.3 encrypted extensions
- + [tls#835](#) dimkr - Added a Meson project
- + [frame#285](#) Marandil - Add explicit parameter variants to ec_*_pub data files
- + [crypto#147](#) BrianSipos - Register Name Constraints extension and BPv7 OIDs
- + [crypto#705](#) Marandil - Fix explicit Elliptic Curve parsing

Recent community activity (thank you!)

Valerio @Nordic

- + merged: crypto#718 valeriosetti - doxygen: use CMake build dir instead of source dir to host generated files
- + merged: crypto#760 valeriosetti - [backport 1.1] doxygen: use CMake build dir instead of source dir to host generated files

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