

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 a focus on security and authentication. The overall scene is filled with faint, glowing lines and dots, creating a sense of a complex digital network or data flow.

arm

# Mbed TLS Tech Forum

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

Janos Follath  
[2026-02-23](#)

# Recent community activity (thank you!)

- + merged: [tls#10589](#) daverodgman - [Backport 3.6] fix error in GCC bswap
- + [crypto#301](#) ilie-halip-nxp - scripts: driver\_templates: call driver init/free
- + [crypto#425](#) ilie-halip-nxp - scripts: driver\_templates: fix few driver wrappers
- + [crypto#538](#) ruiliio - Add support for AES-XTS
- + merged: [crypto#649](#) daverodgman - fix error in GCC bswap

# Recent community activity (thank you!)

Valerio @Nordic

- + `tls#10595` valeriosetti - library: `check_config`: fix required hash algorithms for TLS 1.2
- + merged: `tls#10597` valeriosetti - [backport] library: `check_config`: fix required hash algorithms for TLS 1.2
- + `tls#10599` valeriosetti - [backport] include: fix guard in `asn1write.h`
- + `tls#10591` valeriosetti - library: replace `MBEDTLS_RSA_C` with `PSA_WANT`
- + merged: `crypto#693` valeriosetti - include: fix guard in `asn1write.h`
- + merged: `crypto#688` valeriosetti - include: `adjust_config_derived`: add macros to give RSA capabilities

# Major activities within core team

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

- + Mbed TLS 4.1/TF-PSA-Crypto 1.1 preparations
- + PK module refactoring
- + Prototyping and starting ML-DSA integration
- + Bug bounty program
- + Code size optimization initial investigation

# Release Timeline

- + 1.x/4.x
  - 1.0/4.0 (Oct 2025 – released): New major version
  - 1.1/4.1 (planned for end of March 2026): new LTS version
- 3.6 LTS supported until early 2027
  - 3.6.5 (Oct 2025 - released): Security fixes and bugfixes
  - 3.6.6 (planned for end of March 2026)

arm

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה

ధన్యవాదములు