

The background features a dark blue, futuristic aesthetic. A central image shows a smartphone with a glowing fingerprint scanner. The phone is overlaid with a complex network of white and cyan lines, resembling a circuit board or data flow diagram. Binary code (0s and 1s) is scattered throughout the scene, adding to the technological theme. The overall lighting is cool and high-tech.

arm

# Mbed TLS Tech Forum

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

Janos Follath  
[2026-02-09](#)

# Recent community activity (thank you!)

- + [tls#10589](#) daverodgman - [Backport 3.6] fix error in GCC bswap
- + merged: [tls#10577](#) h1wind - fix: Disabling the MBEDTLS\_SSL\_CLI\_C feature caused a compilation error: unused parameter "ssl".
- + merged: [tls#10514](#) ng-gsmk - mbedtls\_ssl\_get\_alert(): getter for fatal alerts
- + [tls#10572](#) machine-moon - Fix MinGW printf ll macro
- + [crypto#649](#) daverodgman - fix error in GCC bswap
- + [crypto#538](#) ruiliio - Add support for AES-XTS.
- + [crypto#677](#) dannysen - ppc64le: Adding PowerPC support for AES and GCM functions.

# Recent community activity (thank you!)

Valerio @Nordic

- + merged: [tls#10570](#) valeriosetti - mbedtls 4.x does not expose mbedtls\_ecp\_curve\_list()
- + merged: [tls#10581](#) valeriosetti - [backport] Software GCM table calculation buggy with gcc -O3
- + [crypto#615](#) valeriosetti - PK: remove `pk\_can\_do()` -- part 1
- + merged: [crypto#668](#) valeriosetti - Software GCM table calculation buggy with gcc -O3
- + [crypto#673](#) valeriosetti - Only build mbedtls\_rsa\_deduce\_private\_exponent when key generation is enabled

# 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