

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 overlaid with a network of white and cyan lines and small 'x' marks, suggesting a digital or data environment.

arm

# Mbed TLS Tech Forum

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

Janos Follath  
2024-10-07

# Recent community activity (thank you!)

- + #9421 mfil - Implement TLS-Exporter
- + #6556 polhenarejos - XChaCha20 and XChaCha20-Poly1305 support.
- + #5824 polhenarejos - Add support to Ed448 in EdDSA
- + #5823 polhenarejos - Add support for SHA-3 KMAC
- + #5822 polhenarejos - SHA-3 cSHAKE128 and cSHAKE256 support
- + #5821 polhenarejos - SHA-3 SHAKE128 and SHAKE256 support
- + #5819 polhenarejos - Add support for EdDSA with ed25519 curve (pure ed25519, ed25519ctx and ed25519ph)
- + #9218 casaroli - Make local functions and objects static
- + #7977 ivq - Fix doc on GCM API
- + #9371 valeriosetti - psasim: use shared memory as messaging system for client-server communication
- + #9302 valeriosetti - PSA: use static key slots to store keys

# Major activities within core team

<https://github.com/orgs/Mbed-TLS/projects/1>

- + TF-PSA-Crypto — main focus in Q4
  - Splitting files, reworking some interfaces (configuration, platform, ...)
  - <https://github.com/Mbed-TLS/TF-PSA-Crypto>
  - Will become upstream source for crypto in Mbed TLS
- + Mbed TLS 4.0
  - PSA\_CRYPTOC / CLIENT always on
  - Consume TF-PSA-Crypto repository as source of PSA and crypto code
  - Remove some legacy interfaces & features
- + Open for SPAKE2+ reviews (tasks defined on [backlog board](#))

# Release Timeline

- + 4.0 currently aiming for first half of 2025
- + 3.6 LTS supported until early 2027
- + 2.28 LTS ends supported life end of 2024

# TF-PSA-Crypto 1.0 + Mbed TLS 4.0 highlights

- + TLS 1.2: removing finite-field DH, static ECDH, PKCS#1v1.5 RSA encryption, CBC
- + Crypto: removing PKCS#1v1.5 RSA encryption, DES, EC curves smaller than 250 bits
- + Removing all crypto ALT (use PSA drivers instead)
- + Removing low-level crypto APIs (use PSA APIs instead)
  - Removing cipher.h; Keeping parts of md.h and pk.h partially as transition layers
  - Removing direct access to bignum/ECC arithmetic
  - Removing direct access to DRBG

arm

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה

ధన్యవాదములు