

The background features a dark blue, futuristic aesthetic with a glowing blue line that starts from the top left and curves across the frame. In the center, a smartphone is shown with a glowing blue fingerprint scanner on its back. The phone's screen displays a grid of numbers and some text. To the right of the phone, there is a glowing blue fingerprint icon. The overall scene is filled with abstract digital patterns, including binary code (0s and 1s) and various geometric shapes.

arm

Mbed TLS Tech Forum

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

Janos Follath
2024-11-18

Recent community activity (thank you!)

- + #9421 mfil - Implement TLS-Exporter
- + #7977 ivq - Fix doc on GCM API
- + #9423 BhanuPrakash-P - Fix pkcs8 unencrypted private key parsing with Attributes field
- + #9371 valeriosetti - psasim: use shared memory as messaging system for client-server communication
- + #9562 valeriosetti - md: allow dispatch to PSA whenever CRYPTO_CLIENT is enabled

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
- + Mbed TLS 3.6.2
 - Security fix release (CVE-2024-49195)
- + 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
 - o 3.6.1 (Aug 2024): mostly fixes related to TLS 1.3
 - o 3.6.2 (Oct 2024): security fix
 - o 3.6.3 (TBA): will support a PSA key store in builds without malloc
- + 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