



arm

Mbed TLS Tech Forum

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

Janos Follath
[2026-10-05](#)

Recent community activity (thank you!)

Mbed TLS

- + tls#10980 stanleys12 - Bind new TLS 1.3 tickets to the ALPN of the current connection
- + tls#10975 Johnsonajibi - sha256: fold high bits of ilen into total[1] on 64-bit platforms
- + tls#10767 eyupcanakman - Fix mbedtls_x509_dn_gets buffer too small for long DN values
- + tls#10936 v1rtu3x - Fix X.509 certificate profiles to honor MBEDTLS_PK_SIGALG_ECDSA
- + tls#10979 v1rtu3x - Backport: Fix x509 profile pk sigalg 4.1
- + tls#10967 v1rtu3x - Fix TLS 1.3 handshakes with opaque PSKs
- + tls#10978 nvxbug - Reject empty ECDHE ClientKeyExchange before reading its length byte
- + tls#10974 MechatronikMonkey - x509_crt: accept empty AuthorityKeyIdentifier sequence
- + tls#10976 Johnsonajibi - lms/lmots: apply the same output-buffer zeroization consistently
- + tls#10973 saadgodikat - Fix DER certificate output on Windows
- + tls#10928 nvxbug - Backport 3.6: Fix off-by-one over-read in TLS 1.2 ClientHello and CertificateRequest
- + tls#10833 nvxbug - Fix off-by-one over-read in TLS 1.2 ClientHello and CertificateRequest
- + tls#10929 nvxbug - Backport 4.1: Fix off-by-one over-read in TLS 1.2 ClientHello and CertificateRequest
- + tls#10969 barakgut - [3.6] Parenthesize arguments of TLS 1.2 sig/hash alg macros
- + tls#10968 barakgut - Parenthesize arguments of TLS 1.2 sig/hash alg macros
- + tls#10970 barakgut - [4.1] Parenthesize arguments of TLS 1.2 sig/hash alg macros
- + tls#10951 barakgut - Add MBEDTLS_SSL_RUNTIME_CONTENT_LEN and per-connection content lengths
- + tls#10792 nvxbug - Reject out-of-bounds ALPN length in ssl_context_load
- + tls#10959 nvxbug - Validate timestamps in mbedtls_x509write_crt_set_validity
- + 2 + © 2024 Arm
+ tls#6192 greg3844 - Fix CRL with critical extension can't be loaded

Recent community activity (thank you!)

TF-PSA-Crypto

- + frame#323 Thomasdjb - Update test functions with spake2+ related definitions
- + crypto#918 ManoharPaturi - PKCS#5 PBES2: reject iteration counts below 1 and mismatching keyLength
- + crypto#931 jan-bruckner - Add linkage guard to constant_time.h
- + crypto#932 Thomasdjb - fix: psa_sign_message wrongly reject pure EDDSA
- + crypto#934 Johnsonajibi - psa_hash: fix the same 4GiB ilen truncation as upstream mbedtls#10975 (1.1 backport)
- + crypto#933 Johnsonajibi - psa_hash: fix the same 4GiB ilen truncation as upstream mbedtls#10975
- + crypto#920 ManoharPaturi - asn1write: reject NULL integer buffers before dereferencing them
- + crypto#929 v1rtu3x - Add SM4 block cipher core and ECB registration
- + crypto#919 ManoharPaturi - PEM: validate PKCS padding in constant time
- + crypto#817 sigvartmh - SPAKE2+: Implement public key import and export
- + crypto#916 jfdev001 - Backport 1.1: Bump cmake min and remove related conditionals
- + crypto#809 asmclyby - Complete the move of driver wrappers to the dispatch/ directory
- + crypto#915 jfdev001 - Bump cmake min and remove related conditionals
- + crypto#892 v1rtu3x - Enforce hash length in psa_sign_hash and psa_verify_hash

Recent community activity (thank you!)

Valerio (Nordic)

- + merged: [tls#10642](#) valeriosetti - [dev] Replace legacy rsa symbols followup
- + merged: [tls#10971](#) valeriosetti - [4.1] Replace legacy rsa symbols followup
- + [tls#10764](#) valeriosetti - Allow TF-PSA-Crypto path to be specified in CMake and Makefiles
- + merged: [tls#10958](#) valeriosetti - scripts: depends-py: add the possibility to provide a fully custom build-and-test command
- + merged: [tls#10960](#) valeriosetti - [4.1] scripts: depends-py: add the possibility to provide a fully custom build-and-test command
- + [crypto#898](#) valeriosetti - Add support for Blake2 MAC
- + [crypto#927](#) valeriosetti - Add Blake2 built-in driver support
- + [crypto#867](#) valeriosetti - Add support for Blake2s and Blake2b hash algorithms
- + [crypto#928](#) valeriosetti - Add support for Blake2 (hash only) through the PSA Crypto APIs
- + merged: [crypto#911](#) valeriosetti - [dev] tests: host_test: add the possibility to filter test cases on a suite
- + merged: [crypto#917](#) valeriosetti - [1.1] tests: host_test: add the possibility to filter test cases on a suite

Major activities within core team

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

- + ML-DSA integration – PSA API
- + Working on SM3 and BLAKE2
- + Security backlog

Release Timeline

- + 1.x/4.x development
 - 1.2/4.2 released on 2026-07-07
 - 1.3/4.3 targeted for end of October
- + 1.1.x/4.1.x LTS supported until March 2029
 - 1.1.1/4.1.1 released on 2026-07-07
 - 1.1.2/4.1.2 targeted for end of October
- + 3.6 LTS supported until early 2027
 - 3.6.7 released on 2026-07-07
 - 3.6.8 targeted for end of October

arm

Thank You

Danke

Gracias

Grazie

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكرًا

ধন্যবাদ

תודה

ధన్యవాదములు