



arm

Mbed TLS Tech Forum

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

Janos Follath
[2026-10-19](#)

Recent community activity (thank you!)

Mbed TLS I

- + tls#11007 nvxbug - Fix out-of-bounds write in mbedtls_ssl_cookie_write
- + merged: tls#10998 jan-bruckner - Backport 3.6: Add linkage guard to constant_time.h
- + tls#10967 v1rtu3x - Fix TLS 1.3 handshakes with opaque PSKs
- + tls#10983 nvxbug - Reject a CSR whose CertificationRequestInfo is not fully consumed
- + tls#11002 JayOfTheKeyboard - Fix IP SAN handling in cert_write and cert_req
- + merged: tls#10997 subotac - Backport 4.1: Reject overflowing numeric OID components
- + merged: tls#10911 subotac - Reject overflowing numeric OID components
- + merged: tls#10996 subotac - Backport 3.6: Reject overflowing numeric OID components
- + tls#10992 yegorich - [Backport 3.6] Fix the build when <sys/auxv.h> is not available on Linux
- + tls#10852 felipereyesmurcia - Fix buffer overreads on malformed inputs in sample programs
- + tls#10780 asmeilby - Complete the move of TF-PSA-Crypto driver wrappers to dispatch/ directory
- + tls#11004 JayOfTheKeyboard - [3.6] Fix IP SAN handling in cert_write and cert_req
- + tls#11003 JayOfTheKeyboard - [4.1] Fix IP SAN handling in cert_write and cert_req
- + tls#6192 greg3844 - Fix CRL with critical extension can't be loaded
- + merged: tls#10975 Johnsonajibi - sha256: fold high bits of ilen into total[1] on 64-bit platforms
- + merged: tls#10973 saadgodikat - Fix DER certificate output on Windows
- + tls#10995 v1rtu3x - Add tls12 sigalg policy tests 4.1
- + merged: tls#10993 saadgodikat - [4.1] Fix DER certificate output on Windows
- + merged: tls#10994 saadgodikat - [3.6] Fix DER certificate output on Windows

Recent community activity (thank you!)

Mbed TLS II

- + tls#10929 nvxbug - Backport 4.1: Fix off-by-one over-read in TLS 1.2 ClientHello and CertificateRequest
- + tls#10928 nvxbug - Backport 3.6: Fix off-by-one over-read in TLS 1.2 ClientHello and CertificateRequest
- + tls#10457 HaniAmmar - Add functions to export TLS traffic keys and sequence numbers for KTLS integration
- + tls#10113 etienne-lms - Fix build warning related to deprecated DTLS connect ID
- + tls#10112 etienne-lms - [Backport 3.6] Fix build warning related to deprecated DTLS connect ID
- + tls#10978 nvxbug - Reject empty ECDHE ClientKeyExchange before reading its length byte
- + tls#10988 JuliusBairaktaris - [4.1] Test the SHA-256 and SHA-512 crypto extensions with GCC and a fortified libc
- + tls#10986 JuliusBairaktaris - [3.6] sha256, sha512: keep the target CPU when enabling the crypto extensions
- + tls#10987 JuliusBairaktaris - Test the SHA-256 and SHA-512 crypto extensions with GCC and a fortified libc
- + merged: tls#10991 nvxbug - Backport 4.1: Reject out-of-bounds ALPN length in ssl_context_load
- + merged: tls#10792 nvxbug - Reject out-of-bounds ALPN length in ssl_context_load
- + merged: tls#10990 nvxbug - Backport 3.6: Reject out-of-bounds ALPN length in ssl_context_load
- + tls#10985 MechatronikMonkey - Backport 4.1: x509_crt: accept empty AuthorityKeyIdentifier sequence
- + tls#10984 MechatronikMonkey - Backport 3.6: x509_crt: accept empty AuthorityKeyIdentifier sequence
- + tls#10989 JC-000 - Accept a cookie extension in a TLS 1.3 HelloRetryRequest
- + tls#10974 MechatronikMonkey - x509_crt: accept empty AuthorityKeyIdentifier sequence
- + frame#307 asnellby - scripts: Add dispatch include path and new generation location
- + frame#324 v1rtu3x - generate_psa_tests: skip ML-DSA key types

Recent community activity (thank you!)

TF-PSA-Crypto

- + merged: crypto#940 jan-bruckner - Backport 1.1: Add linkage guard to constant_time.h
- + crypto#931 jan-bruckner - Add linkage guard to constant_time.h
- + crypto#892 v1rtu3x - Enforce hash length in psa_sign_hash and psa_verify_hash
- + crypto#730 hasheddan - docs: fix broken links between specifications
- + crypto#809 asnellby - Complete the move of driver wrappers to the dispatch/ directory
- + crypto#946 brandon-arrendondo - cipher: bound the zeroize in mbedtls_cipher_check_tag()
- + crypto#938 yegorich - Fix the build when <sys/auxv.h> is not available on Linux
- + crypto#873 sweetlilmre - constant_time: fix the -Os inlining loss, and add an Xtensa assembly path
- + crypto#538 ruilio - Add support for AES-XTS
- + crypto#939 yegorich - Add AES-XTS support to the PSA built-in driver
- + merged: crypto#934 Johnsonajibi - psa_hash: fix the same 4GiB ilen truncation as upstream mbedtls#10975 (1.1 backport)
- + merged: crypto#933 Johnsonajibi - psa_hash: fix the same 4GiB ilen truncation as upstream mbedtls#10975
- + crypto#929 v1rtu3x - Add SM4 block cipher core and ECB registration
- + crypto#936 JuliusBairaktaris - sha256, sha512: keep the target CPU when enabling the crypto extensions
- + crypto#937 JuliusBairaktaris - [1.1] sha256, sha512: keep the target CPU when enabling the crypto extensions
- + crypto#935 v1rtu3x - Support the ML-DSA-87 public key type through the PSA API
- + crypto#927 valeriosetti - Add Blake2 built-in driver support
- + crypto#928 valeriosetti - Add support for Blake2 (hash only) through the PSA Crypto APIs

Announcement

Future Maintenance of Mbed TLS

- + Existing Mbed TLS maintainers are ramping down their effort on TLS and X.509 libraries.
- + From April 2027, existing maintainers will cease development and maintenance of TLS and X.509 libraries.
- + Security incident response, security fixes and releases will cease from April 2027, unless new maintainers have joined the project and ramped up by then.
- + Existing maintainers will continue development and maintenance of TF-PSA-Crypto.

If you or your organisation are interested in contributing to the future maintenance of Mbed TLS, please contact mbed-tls-owner@lists.trustedfirmware.org.

Major activities within core team

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

- + ML-DSA integration – PSA API
- + Security backlog
- + Code Size optimization
- + Project split
 - CI
 - Framework

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