



CycloneSSL is a lightweight TLS / DTLS implementation targeted for use by embedded application developers. It provides the ability to secure communications over the Internet (e.g. IoT protocols, electronic mail, web server, file transfer, VoIP).

HTTP	HTTP/2	MQTT	MQTT-SN	CoAP	FTP	SMTP	7 - Application
TLS Handshake Protocol		TLS Change Cipher Spec Protocol		TLS Alert Protocol		Application Data	6 - Presentation
TLS Record Protocol			DTLS Record Protocol				
Socket							5 - Session

Main Features

- Server and/or client operation
- Supports TLS 1.0, TLS 1.1, TLS 1.2 and TLS 1.3 protocols
- Supports DTLS 1.0 and DTLS 1.2 (Datagram Transport Layer Security)
- Supports QUIC transport layer
- Robust and efficient implementation
- Supports ECC (Elliptic Curve Cryptography)
- Rich set of TLS cipher suites (including Suite B and CNSA profiles)
- RSA, Diffie-Hellman and ECDH key exchange algorithms
- Post-quantum key agreement
- Compliant with BSD socket API
- Flexible memory footprint. Built-time configuration to embed only the necessary features
- Consistent application programming interface (API)
- Portable architecture (no processor dependencies)
- The library is distributed as a full ANSI C and highly maintainable source code

Supported Algorithms

- ECDH key exchange based on Curve25519 (X25519) and Curve448 (X448)
- FFDHE (Finite Field Diffie-Hellman Ephemeral)
- ML-KEM post-quantum key exchange algorithms (ML-KEM-512, ML-KEM-768 and ML-KEM-1024)
- PQ-hybrid key exchange algorithms (SecP256r1MLKEM768, SecP384r1MLKEM1024 and X25519MLKEM768)
- Supports PSK (Pre-Shared Key) cipher suites
- RSA signature schemes (RSASSA PKCS#1 v1.5 and RSASSA-PSS)
- DSA and ECDSA signature schemes
- EdDSA signature scheme (Ed25519 and Ed448 elliptic curves)
- Supports stream ciphers and CBC block ciphers
- Cipher Block Chaining-MAC (CCM) and Galois Counter Mode (GCM)
- ChaCha20Poly1305 Authenticated Encryption with Associated Data (AEAD)
- Supports AES, Camellia, SEED and ARIA encryption algorithms
- Legacy support for RC4, IDEA, DES and 3DES encryption algorithms
- Supports SHA-256, SHA-384 and SHA-512 hash algorithms
- Legacy support for MD5 and SHA-1 hash algorithms
- Supports ShangMi (SM) cipher suites for TLS 1.3
- Session resumption mechanism
- Session ticket mechanism (RFC 5077)
- Supports secure renegotiation (RFC 5746)
- TLS channel binding (RFC 5929)
- Fallback SCSV signaling cipher suite
- SNI extension (Server Name Indication)
- Raw Public Keys (RFC 7250)
- Maximum Fragment Length extension (RFC 6066)
- Record Size Limit extension (RFC 8449)
- Application-Layer Protocol Negotiation (ALPN) extension
- Encrypt-Then-MAC extension
- Extended Master Secret extension
- ClientHello Padding extension (RFC 7685)
- (EC)DHE and PSK key establishment (TLS 1.3)
- Middlebox compatibility mode (TLS 1.3)
- Key update mechanism (TLS 1.3)
- Early data (TLS 1.3 client)
- X.509 certificate parsing and PKIX path validation
- Parsing of public/private keys (PKCS #1 and PKCS #8 formats supported)
- Parsing of encrypted private keys (PKCS #1 and PKCS #8 formats supported)

Supported Extensions

- session_ticket (RFC 5077)
- renegotiation_info (RFC 5746)
- server_name (RFC 6066)
- max_fragment_length (RFC 6066)
- trusted_ca_keys (RFC 6066)
- client_certificate_type (RFC 7250)
- server_certificate_type (RFC 7250)
- application_layer_protocol_negotiation (RFC 7301)
- encrypt_then_mac (RFC 7366)
- extended_master_secret (RFC 7627)
- padding (RFC 7685)
- supported_groups (RFC 7919)
- ec_point_formats (RFC 8422)
- signature_algorithms (RFC 8446)
- pre_shared_key (RFC 8446)
- early_data (RFC 8446)
- supported_versions (RFC 8446)
- cookie (RFC 8446)
- psk_key_exchange_modes (RFC 8446)
- certificate_authorities (RFC 8446)
- signature_algorithms_cert (RFC 8446)
- key_share (RFC 8446)
- record_size_limit (RFC 8449)
- quic_transport_parameters (RFC 9001)

RFC

- RFC 2246: The TLS Protocol Version 1.0
- RFC 3268: Advanced Encryption Standard (AES) Cipher Suites for TLS
- RFC 4162: Addition of SEED Cipher Suites to Transport Layer Security (TLS)
- RFC 4279: Pre-Shared Key Cipher Suites for Transport Layer Security (TLS)
- RFC 4346: The Transport Layer Security (TLS) Protocol Version 1.1
- RFC 4347: Datagram Transport Layer Security (DTLS)
- RFC 4492: Elliptic Curve Cryptography (ECC) Cipher Suites for TLS
- RFC 5077: Transport Layer Security (TLS) Session Resumption without Server-Side State
- RFC 5116: An Interface and Algorithms for Authenticated Encryption
- RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- RFC 5288: AES Galois Counter Mode (GCM) Cipher Suites for TLS
- RFC 5289: TLS ECC Cipher Suites with SHA-256/384 and AES Galois Counter Mode
- RFC 5469: DES and IDEA Cipher Suites for Transport Layer Security (TLS)
- RFC 5487: PSK Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode
- RFC 5489: ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)
- RFC 5746: TLS Renegotiation Indication Extension
- RFC 5929: Channel Bindings for TLS
- RFC 5932: Camellia Cipher Suites for TLS
- RFC 6066: Transport Layer Security (TLS) Extensions: Extension Definitions
- RFC 6101: The Secure Sockets Layer (SSL) Protocol Version 3.0
- RFC 6176: Prohibiting Secure Sockets Layer (SSL) Version 2.0
- RFC 6209: Addition of the ARIA Cipher Suites to Transport Layer Security (TLS)
- RFC 6347: Datagram Transport Layer Security Version 1.2
- RFC 6367: Addition of the Camellia Cipher Suites to Transport Layer Security (TLS)
- RFC 6460: Suite B Profile for Transport Layer Security (TLS)
- RFC 6655: AES-CCM Cipher Suites for Transport Layer Security (TLS)
- RFC 7027: Elliptic Curve Cryptography (ECC) Brainpool Curves for TLS
- RFC 7250: Using Raw Public Keys in TLS and DTLS
- RFC 7251: AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS
- RFC 7301: TLS Application-Layer Protocol Negotiation Extension
- RFC 7366: Encrypt-then-MAC for TLS and DTLS
- RFC 7465: Prohibiting RC4 Cipher Suites
- RFC 7507: TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks
- RFC 7525: Recommendations for Secure Use of TLS and DTLS
- RFC 7539: ChaCha20 and Poly1305 for IETF Protocols
- RFC 7568: Deprecating Secure Sockets Layer Version 3.0
- RFC 7627: TLS Session Hash and Extended Master Secret Extension
- RFC 7685: A Transport Layer Security (TLS) ClientHello Padding Extension
- RFC 7905: ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS)
- RFC 7919: Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for TLS
- RFC 8422: ECC Cipher Suites for TLS Versions 1.2 and Earlier
- RFC 8442: ECDHE_PSK with AES-GCM and AES-CCM Cipher Suites for TLS 1.2 and DTLS 1.2
- RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3
- RFC 8447: IANA Registry Updates for TLS and DTLS
- RFC 8449: Record Size Limit Extension for TLS
- RFC 8734: Elliptic Curve Cryptography (ECC) Brainpool Curves for TLS Version 1.3
- RFC 8996: Deprecating TLS 1.0 and TLS 1.1
- RFC 8998: ShangMi (SM) Cipher Suites for TLS 1.3
- RFC 9001: Using TLS to Secure QUIC
- RFC 9150: TLS 1.3 Authentication and Integrity-Only Cipher Suites
- RFC 9151: Commercial National Security Algorithm (CNSA) Suite Profile for TLS and DTLS 1.2 and 1.3
- RFC 9155: Deprecating MD5 and SHA-1 Signature Hashes in TLS 1.2 and DTLS 1.2
- RFC 9325: Recommendations for Secure Use of TLS and DTLS
- RFC draft: ML-KEM Post-Quantum Key Agreement for TLS 1.3
- RFC draft: Hybrid key exchange in TLS 1.3
- RFC draft: Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3
- RFC draft: Hybrid Post-quantum Key Exchange SM2-MLKEM for TLSv1.3
- RFC draft: The SSLKEYLOGFILE Format for TLS

NIST

- SP 800-52: Guidelines for the Selection and Use of TLS Implementations

Supported Processors

- ARM Cortex-M3
- ARM Cortex-M4
- ARM Cortex-M7
- ARM Cortex-M33
- ARM Cortex-M55
- ARM Cortex-M85
- ARM Cortex-R4
- ARM Cortex-A5
- ARM Cortex-A7
- ARM Cortex-A8
- ARM Cortex-A9
- ARM Cortex-A55
- RISC-V
- MIPS M4K
- MIPS microAptiv / M-Class
- Infineon TriCore AURIX
- PowerPC e200
- Coldfire V2
- RX600
- AVR32
- Xtensa LX6

Supported Operating Systems

- Amazon FreeRTOS
- SafeRTOS
- ChibiOS/RT
- CMSIS-RTOS
- CMSIS-RTOS2
- CMX-RTX
- Keil RTXv4 and RTXv5
- Micrium μ C/OS-II and μ C/OS-III
- Eclipse ThreadX
- PX5 RTOS
- Segger embOS
- TI-RTOS (SYS/BIOS)
- Zephyr RTOS
- Bare Metal programming (without RTOS)

Supported Compilers / Toolchains

Toolchain / IDE	Compiler
Makefile	GCC
AC6 System Workbench for STM32 (SW4STM32)	GCC
Atollic TrueSTUDIO	GCC
Espressif ESP-IDF	GCC
HighTec Toolset for TriCore	GCC
IAR Embedded Workbench	EWARM, EWRX
Infineon DAVE	GCC
Keil MDK-ARM	ARM Compiler v5, ARM Compiler v6 (CLANG)
Microchip Studio (Atmel Studio)	GCC
Microchip MPLAB X	GCC, XC32
Microsoft Visual Studio	MSVC
NXP MCUXpresso	GCC
NXP S32 Design Studio (S32DS)	GCC
Renesas e2Studio	GCC, CC-RX
Segger Embedded Studio	GCC
ST STM32CubeIDE	GCC
Tasking VX-Toolset	VX-Toolset for TriCore
TI Code Composer Studio (CSS)	GCC, ARM-CGT