



## CycloneSSL

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).

### 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)
- Legacy support for SSL 3.0
- Robust and efficient implementation
- Supports ECC (Elliptic Curve Cryptography)
- Rich set of TLS cipher suites (including Suite B profile)
- RSA, Diffie-Hellman and ECDH key exchange algorithms
- 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)
- 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 RC4, IDEA, DES, 3DES, AES, Camellia, SEED and ARIA encryption algorithms
- Supports MD5, SHA-1, SHA-256, SHA-384 and SHA-512 hash algorithms
- Session resumption mechanism
- Session ticket mechanism
- Supports secure renegotiation
- 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
- Extended Master Secret extension
- ClientHello Padding extension (RFC 7685)
- (EC)DHE key establishment (TLS 1.3)
- PSK key establishment (TLS 1.3)
- PSK with (EC)DHE 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 certificates and PKIX path validation

## Supported Processors

- ARM7TDMI / ARM926EJ-S
- ARM Cortex-M3
- ARM Cortex-M4
- ARM Cortex-M7
- ARM Cortex-R4
- ARM Cortex-A5
- ARM Cortex-A8
- ARM Cortex-A9
- RISC-V
- MIPS M4K
- MIPS microAptiv
- PowerPC e200
- Coldfire V2
- RX600
- AVR32
- Xtensa LX6

## Supported Compilers / Toolchains

- GNU GCC / Makefile
- Atollic TrueSTUDIO
- IAR Embedded Workbench
- Keil MDK-ARM
- Microsoft Visual Studio
- Segger Embedded Studio
- AC6 System Workbench for STM32 (SW4STM32)
- Atmel Studio
- Infineon DAVE
- Microchip MPLAB X
- NXP MCUXpresso
- Renesas e2Studio
- ST STM32CubeIDE
- TI Code Composer Studio (CSS)

## Supported Operating Systems

- Amazon FreeRTOS
- ChibiOS/RT
- CMSIS-RTOS
- CMSIS-RTOS2 (RTX v5 and FreeRTOS)
- Keil RTX
- Micrium  $\mu$ C/OS-II
- Micrium  $\mu$ C/OS-III
- Segger embOS
- SYS/BIOS (TI-RTOS)
- Bare Metal programming (without RTOS)

## 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 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 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 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 7507](#): TLS Fallback Signaling Cipher Suite Value (SCSV)
- [RFC 7525](#): Recommendations for Secure Use of TLS and DTLS
- [RFC 7539](#): ChaCha20 and Poly1305 for IETF Protocols
- [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
- [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 draft](#): TLS 1.3 Authentication and Integrity only Cipher Suites (version 6)

## NIST

- [SP 800-52](#): Guidelines for the Selection and Use of TLS Implementations