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). CycloneSSL implements all the necessary cryptographic features to make your application safe and secure. CycloneSSL is available either as open source (GPLv2) or under a commercial license.

Main Features

- Server and/or client operation
- TLS 1.0, 1.1, 1.2 and TLS 1.3 support
- DTLS 1.0 and 1.2 support
- 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, ECDHE and PSK key exchange algorithms
- Supports stream ciphers and block ciphers (RC4, IDEA, DES, 3DES, AES, Camellia, SEED and ARIA)
- Supports MD5, SHA-1, SHA-256, SHA-384 and SHA-512 hash algorithms
- Supports CBC, GCM, CCM and CCM_8 cipher modes
- ChaCha20Poly1305 AEAD cipher
- RSA, RSA-PSS, DSA, ECDSA and EdDSA signature schemes
- Session resumption mechanism
- SNI (Server Name Indication) extension
- ALPN (Application-Layer Protocol Negotiation) extension
- Maximum Fragment Length extension
- Record Size Limit extension
- Extended Master Secret extension
- ClientHello Padding extension
- Supports Raw Public Keys (RPK)
- Session ticket mechanism (TLS 1.3)
- (EC)DHE key establishment (TLS 1.3)
- PSK key establishment (TLS 1.3)
- Middlebox compatibility mode (TLS 1.3)
- Key update mechanism (TLS 1.3)
- Early data (TLS 1.3 client)
- Secure renegotiation
- Fallback SCSV signaling cipher suite
- FFDHE (Finite Field Diffie-Hellman Ephemeral)
- PKIX path validation
- Flexible memory footprint. Built-time configuration to embed only the necessary features
- Consistent application programming interface (API)
- Portable architecture (no processor dependencies)
- Debugging and trace functionality to ease development and integration
- The library is distributed as a full ANSI C and highly maintainable source code
- Dual licensing (open source or commercial license)

Supported Devices

- ARM7TDMI®
- ARM926EJ-S™
- Cortex™-M3/M4/M7
- Cortex™-A5/A8/A9
- APS1 / APS3 / APS3R / APS5 / FPS6
- AVR32
- PIC32
- RX600
- Xtensa LX6

Supported Elliptic curves

- curve25519 (X25519)
- curve448 (X448)
- Ed25519
- Ed448
- secp160r1
- secp192r1 (NIST P-192)
- secp224r1 (NIST P-224)
- secp256r1 (NIST P-256)
- secp384r1 (NIST P-384)
- secp521r1 (NIST P-521)
- brainpoolP256r1
- brainpoolP384r1
- brainpoolP512r1

Supported Cipher Suites

TLS 1.3 cipher suites:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_CCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_CHACHA20_POLY1305_SHA256

RSA cipher suites:

- TLS_RSA_WITH_RC4_128_MD5 (†)
- TLS_RSA_WITH_RC4_128_SHA (†)
- TLS_RSA_WITH_IDEA_CBC_SHA (†)
- TLS_RSA_WITH_DES_CBC_SHA (†)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (w)
- TLS_RSA_WITH_AES_128_CBC_SHA (w)
- TLS_RSA_WITH_AES_256_CBC_SHA (w)
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CCM
- TLS_RSA_WITH_AES_256_CCM
- TLS_RSA_WITH_AES_128_CCM_8
- TLS_RSA_WITH_AES_256_CCM_8
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (w)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (w)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384
- TLS_RSA_WITH_SEED_CBC_SHA (w)
- TLS_RSA_WITH_ARIA_128_CBC_SHA256
- TLS_RSA_WITH_ARIA_256_CBC_SHA384
- TLS_RSA_WITH_ARIA_128_GCM_SHA256
- TLS_RSA_WITH_ARIA_256_GCM_SHA384
- TLS_RSA_WITH_NULL_MD5 (†)
- TLS_RSA_WITH_NULL_SHA (†)
- TLS_RSA_WITH_NULL_SHA256 (†)

DHE-RSA cipher suites:

- TLS_DHE_RSA_WITH_DES_CBC_SHA (†)
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (w)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (w)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (w)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CCM
- TLS_DHE_RSA_WITH_AES_256_CCM
- TLS_DHE_RSA_WITH_AES_128_CCM_8
- TLS_DHE_RSA_WITH_AES_256_CCM_8
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (w)
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (w)
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
- TLS_DHE_RSA_WITH_SEED_CBC_SHA (w)
- TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384
- TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256
- TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256

ECDHE-RSA cipher suites:

- TLS_ECDHE_RSA_WITH_RC4_128_SHA (†)
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (w)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (w)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (w)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_NULL_SHA (†)

ECDHE-ECDSA cipher suites:

- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (†)
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (w)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (w)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (w)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8
- TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_ECDSA_WITH_NULL_SHA (†)

DHE-DSS cipher suites:

- TLS_DHE_DSS_WITH_DES_CBC_SHA (†)
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (w)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA (w)
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA (w)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
- TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA (w)
- TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA (w)
- TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256
- TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384
- TLS_DHE_DSS_WITH_SEED_CBC_SHA (w)
- TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256
- TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384
- TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256
- TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384

Supported Cipher Suites (continued)

PSK cipher suites:

- TLS_PSK_WITH_RC4_128_SHA (†)
- TLS_PSK_WITH_3DES_EDE_CBC_SHA (w)
- TLS_PSK_WITH_AES_128_CBC_SHA (w)
- TLS_PSK_WITH_AES_256_CBC_SHA (w)
- TLS_PSK_WITH_AES_128_CBC_SHA256
- TLS_PSK_WITH_AES_256_CBC_SHA384
- TLS_PSK_WITH_AES_128_GCM_SHA256
- TLS_PSK_WITH_AES_256_GCM_SHA384
- TLS_PSK_WITH_AES_128_CCM
- TLS_PSK_WITH_AES_256_CCM
- TLS_PSK_WITH_AES_128_CCM_8
- TLS_PSK_WITH_AES_256_CCM_8
- TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256
- TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384
- TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256
- TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384
- TLS_PSK_WITH_ARIA_128_CBC_SHA256
- TLS_PSK_WITH_ARIA_256_CBC_SHA384
- TLS_PSK_WITH_ARIA_128_GCM_SHA256
- TLS_PSK_WITH_ARIA_256_GCM_SHA384
- TLS_PSK_WITH_CHACHA20_POLY1305_SHA256
- TLS_PSK_WITH_NULL_SHA (†)
- TLS_PSK_WITH_NULL_SHA256 (†)
- TLS_PSK_WITH_NULL_SHA384 (†)

DHE-PSK cipher suites:

- TLS_DHE_PSK_WITH_RC4_128_SHA (†)
- TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA (w)
- TLS_DHE_PSK_WITH_AES_128_CBC_SHA (w)
- TLS_DHE_PSK_WITH_AES_256_CBC_SHA (w)
- TLS_DHE_PSK_WITH_AES_128_CBC_SHA256
- TLS_DHE_PSK_WITH_AES_256_CBC_SHA384
- TLS_DHE_PSK_WITH_AES_128_GCM_SHA256
- TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
- TLS_DHE_PSK_WITH_AES_128_CCM
- TLS_DHE_PSK_WITH_AES_256_CCM
- TLS_DHE_PSK_WITH_AES_128_CCM_8
- TLS_DHE_PSK_WITH_AES_256_CCM_8
- TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384
- TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256
- TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384
- TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256
- TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384
- TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256
- TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384
- TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256
- TLS_DHE_PSK_WITH_NULL_SHA (†)
- TLS_DHE_PSK_WITH_NULL_SHA256 (†)
- TLS_DHE_PSK_WITH_NULL_SHA384 (†)

RSA-PSK cipher suites:

- TLS_RSA_PSK_WITH_RC4_128_SHA (†)
- TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA (w)
- TLS_RSA_PSK_WITH_AES_128_CBC_SHA (w)
- TLS_RSA_PSK_WITH_AES_256_CBC_SHA (w)
- TLS_RSA_PSK_WITH_AES_128_CBC_SHA256
- TLS_RSA_PSK_WITH_AES_256_CBC_SHA384
- TLS_RSA_PSK_WITH_AES_128_GCM_SHA256
- TLS_RSA_PSK_WITH_AES_256_GCM_SHA384
- TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384
- TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256
- TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384
- TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256
- TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384
- TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256
- TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384
- TLS_RSA_PSK_WITH_CHACHA20_POLY1305_SHA256
- TLS_RSA_PSK_WITH_NULL_SHA (†)
- TLS_RSA_PSK_WITH_NULL_SHA256 (†)
- TLS_RSA_PSK_WITH_NULL_SHA384 (†)

DH-anon cipher suites:

- TLS_DH_anon_WITH_RC4_128_MD5 (†)
- TLS_DH_anon_WITH_DES_CBC_SHA (†)
- TLS_DH_anon_WITH_3DES_EDE_CBC_SHA (†)
- TLS_DH_anon_WITH_AES_128_CBC_SHA (†)
- TLS_DH_anon_WITH_AES_256_CBC_SHA (†)
- TLS_DH_anon_WITH_AES_128_CBC_SHA256 (†)
- TLS_DH_anon_WITH_AES_256_CBC_SHA256 (†)
- TLS_DH_anon_WITH_AES_128_GCM_SHA256 (†)
- TLS_DH_anon_WITH_AES_256_GCM_SHA384 (†)
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA (†)
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA (†)
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256 (†)
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256 (†)
- TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256 (†)
- TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384 (†)
- TLS_DH_anon_WITH_SEED_CBC_SHA (†)
- TLS_DH_anon_WITH_ARIA_128_CBC_SHA256 (†)
- TLS_DH_anon_WITH_ARIA_256_CBC_SHA384 (†)
- TLS_DH_anon_WITH_ARIA_128_GCM_SHA256 (†)
- TLS_DH_anon_WITH_ARIA_256_GCM_SHA384 (†)

ECDHE-PSK cipher suites:

- TLS_ECDHE_PSK_WITH_RC4_128_SHA (†)
- TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA (w)
- TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA (w)
- TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA (w)
- TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256
- TLS_ECDHE_PSK_WITH_AES_128_CCM_8_SHA256
- TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256
- TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384
- TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256
- TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384
- TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_PSK_WITH_NULL_SHA (†)
- TLS_ECDHE_PSK_WITH_NULL_SHA256 (†)
- TLS_ECDHE_PSK_WITH_NULL_SHA384 (†)

ECDH-anon cipher suites:

- TLS_ECDH_anon_WITH_RC4_128_SHA (†)
- TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA (†)
- TLS_ECDH_anon_WITH_AES_128_CBC_SHA (†)
- TLS_ECDH_anon_WITH_AES_256_CBC_SHA (†)
- TLS_ECDH_anon_WITH_NULL_SHA (†)

(†) denotes insecure cipher suites
(w) denotes weak cipher suites

Reference Standards

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

NIST

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

