CycloneIPSEC

CycloneIPSEC is an IPsec / IKEv2 library designed for embedded applications. IPsec is a suite of protocols used to implement secure communication between two sites over the Internet. IPsec operates at the network layer of the OSI model. The main protocols comprising IPsec are AH (Authentication Header), ESP (Encapsulating Security Payload) and IKEv2 (Internet Key Exchange version 2). AH provides data integrity protection while ESP provides both confidentiality and data integrity protection. IKEv2 is the protocol used to manage security associations between two entities.

Main Features

- AH (Authentication Header) implementation
- ESP (Encapsulating Security Payload) implementation
- IKEv2 (Internet Key Exchange version 2) implementation
- Supports Transport mode over IPv4 (Tunnel mode is not supported)
- Pre-shared key and certificate authentication methods
- Key exchange using Diffie-Hellman, ECDH, Curve25519 and Curve448 algorithms
- RSA, RSA-PSS, DSA, ECDSA, Ed25519 and Ed448 signature algorithms
- AES, Camellia and ChaCha20Poly1305 encryption algorithms
- Legacy support for IDEA, DES and 3DES encryption algorithms
- CBC, CTR, CCM and GCM encryption modes
- SHA-256, SHA-384 and SHA-512 hash algorithms
- Legacy support for MD5, SHA-1 and Tiger hash algorithms
- Commercial National Security Algorithm (CNSA) suite cryptography
- Anti-replay mechanism with configurable sliding window size (64 by default)
- HMAC, CMAC and XCBC-MAC integrity algorithms
- Supportes ESNs (Extended Sequence Numbers)
- Cookie generation and verification
- Supports Digital Signature method
- Supports SIGNATURE_HASH_ALGORITHMS and INITIAL_CONTACT notifications
- Supports DPD (Dead Peer Detection) mechanism
- Flexible memory footprint. Built-time configuration to embed only the necessary features
- Portable architecture (no processor dependencies)
- The library is distributed as a full ANSI C and highly maintainable source code

Key Exchange Methods

- 768-bit MODP Group(†)
- 1024-bit MODP Group(w)
- 1536-bit MODP Group(w)
- 2048-bit MODP Group
- 3072-bit MODP Group
- 4096-bit MODP Group
- 6144-bit MODP Group
- 8192-bit MODP Group
- 192-bit random ECP Group
- 224-bit random ECP Group
- 256-bit random ECP Group
- 384-bit random ECP Group
- 521-bit random ECP Group
- 224-bit Brainpool ECP Group
- 256-bit Brainpool ECP Group
- 384-bit Brainpool ECP Group
- 512-bit Brainpool ECP Group
- Curve25519
- Curve448

Authentication Methods

- Shared Key Message Integrity Code
- RSA Digital Signature
- DSS Digital Signature
- ECDSA with SHA-256 on P-256 Curve
- ECDSA with SHA-384 on P-384 Curve
- ECDSA with SHA-512 on P-521 Curve
- Digital Signature

Pseudorandom Functions

- PRF_HMAC_MD5(†)
- PRF_HMAC_SHA1(w)
- PRF_HMAC_TIGER(w)
- PRF_HMAC_SHA2_256
- PRF_HMAC_SHA2_384
- PRF_HMAC_SHA2_512
- PRF_AES128_CMAC
- PRF_AES128_XCBC

Encryption Algorithms

- ENCR_IDEA(†)
- ENCR_DES(†)
- ENCR_3DES(w)
- ENCR_AES_CBC
- ENCR_AES_CTR
- ENCR_AES_CCM_8
- ENCR_AES_CCM_12
- ENCR_AES_CCM_16
- ENCR_AES_GCM_8
- ENCR_AES_GCM_12
- ENCR_AES_GCM_16
- ENCR_CAMELLIA_CBC
- ENCR_CAMELLIA_CTR
- ENCR_CAMELLIA_CCM_8
- ENCR_CAMELLIA_CCM_12
- ENCR_CAMELLIA_CCM_16
- ENCR_CHACHA20_POLY1305

Integrity Algorithms

- AUTH_HMAC_MD5_96(†)
- AUTH_HMAC_SHA1_96(w)
- AUTH_HMAC_SHA2_256_128
- AUTH_HMAC_SHA2_384_192
- AUTH_HMAC_SHA2_512_256
- AUTH_AES_CMAC_96
- AUTH_AES_XCBC_96

(†) denotes insecure algorithms

(w) denotes weak algorithms

IPsec Core

- RFC 4301: Security Architecture for the Internet Protocol
- RFC 4302: IP Authentication Header
- RFC 4303: IP Encapsulating Security Payload (ESP)

IPsec Extensions

- RFC 2451: The ESP CBC-Mode Cipher Algorithms
- RFC 3566: The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
- RFC 3602: The AES-CBC Cipher Algorithm and Its Use with IPsec
- RFC 3686: Using Advanced Encryption Standard (AES) Counter Mode With IPsec ESP
- RFC 4106: The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
- RFC 4308: Cryptographic Suites for IPsec
- RFC 4309: Using Advanced Encryption Standard (AES) CCM Mode with IPsec ESP
- RFC 4494: The AES-CMAC-96 Algorithm and Its Use with IPsec
- RFC 4868: Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
- RFC 5529: Modes of Operation for Camellia for Use with IPsec
- RFC 6379: Suite B Cryptographic Suites for IPsec
- RFC 6380: Suite B Profile for Internet Protocol Security (IPsec)
- RFC 7634: ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol (IKE) and IPsec
- RFC 8221: Cryptographic Algorithm Implementation Requirements and Usage Guidance for ESP and AH
- RFC 9206: Commercial National Security Algorithm (CNSA) Suite Cryptography for IPsec

IKE Core

- RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2)

IKE Extensions

- RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 4307: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4434: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4615: The AES-CMAC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4718: IKEv2 Clarifications and Implementation Guidelines
- RFC 4753: ECP Groups For IKE and IKEv2
- RFC 4754: IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)
- RFC 4945: The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX
- RFC 5282: Using Authenticated Encryption Algorithms with the Encrypted Payload of the IKEv2 Protocol
- RFC 5903: Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2
- RFC 5930: Using Advanced Encryption Standard Counter Mode (AES-CTR) with the IKEv2 Protocol
- RFC 6932: Brainpool Elliptic Curves for the Internet Key Exchange (IKE) Group Description Registry
- RFC 6954: Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for the IKEv2
- RFC 6989: Additional Diffie-Hellman Tests for the IKEv2
- RFC 7427: Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)
- RFC 7815: Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation
- RFC 8031: Curve25519 and Curve448 for the IKEv2 Key Agreement
- RFC 8247: Algorithm Implementation Requirements and Usage Guidance for the IKEv2
- RFC 8420: Using the Edwards-Curve Digital Signature Algorithm (EdDSA) in the IKEv2
- RFC 9395: Deprecation of the IKEv1 Protocol and Obsoleted Algorithms
- RFC 9827: Renaming the Extended Sequence Numbers (ESN) Transform Type in the IKEv2

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 µC/OS-II and µC/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