



CycloneEST is an EST (Enrollment over Secure Transport) client implementation designed for embedded applications. EST is a certificate management protocol that provides a secure method for IoT devices to enroll for X.509 certificates over HTTPS. EST automates certificate provisioning and renewal, ensuring secure device identities without requiring manual intervention.

Main Features

- EST protocol implementation as per RFC 7030
- Client mode of operation
- Certificate management (enrollment and re-enrollment operations)
- Supports RSA and ECDSA certificates
- Supports HTTP Basic and Digest authentication
- Supports TLS Channel Binding for linking identity and proof-of-possession
- Comprehensive user API
- 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

Reference Standards

- [RFC 7030](#): Enrollment over Secure Transport
- [RFC 2315](#): PKCS #7: Cryptographic Message Syntax Version 1.5
- [RFC 2986](#): PKCS #10: Certification Request Syntax Specification Version 1.7
- [RFC 5929](#): Channel Bindings for TLS

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