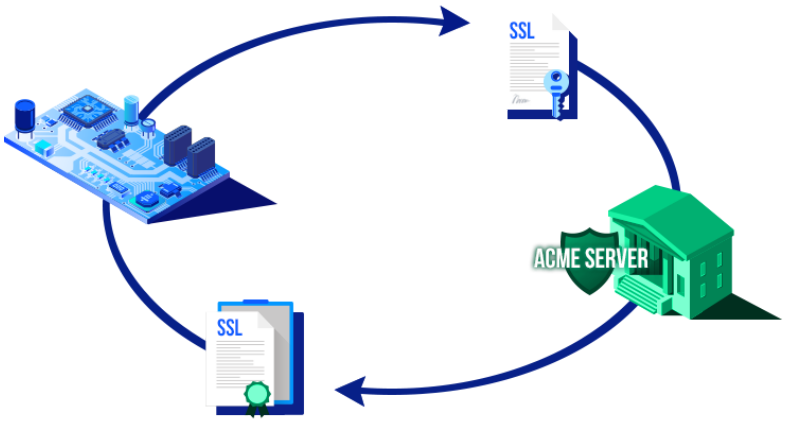
CycloneACME

CycloneACME is an ACME (Automatic Certificate Management Environment) client implementation designed for embedded applications. It can be used to automate the management of X.509 certificates, including ordering, renewing, and revoking them, with a remote certification authority like Let's Encrypt. ACME enables the deployment of public-key infrastructure on Internet-facing devices, such as HTTPS servers, at a very low cost.



Main Features

- ACME v2 protocol implementation
- Client mode of operation
- ACME account management (creation, update, deactivation and key rollover)
- Certificate management (ordering, renewal and revocation)
- Supports RSA, ECDSA and EdDSA certificates
- Supports standard ACME challenges (HTTP, DNS and TLS-ALPN)
- ACME-DNS client provides a simple way to automate ACME DNS challenges
- Compatible with ACME servers such as Let's Encrypt, Encryption Everywhere or Buypass Go SSL
- 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

Supported ACME Challenges

- http-01 (HTTP-based challenge type)
- tls-alpn-01 (TLS-based challenge type)
- dns-01 (DNS-based challenge type)

Supported Signature Algorithms

- RSA
- ECDSA
- Ed25519
- Ed448

Reference Standards

- RFC 8555: Automatic Certificate Management Environment (ACME)
- RFC 8737: ACME TLS Application-Layer Protocol Negotiation (ALPN) Challenge Extension
- RFC 7515: JSON Web Signature (JWS)
- RFC 7517: JSON Web Key (JWK)
- RFC 7518: JSON Web Algorithms (JWA)
- RFC 7638: JSON Web Key (JWK) Thumbprint

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