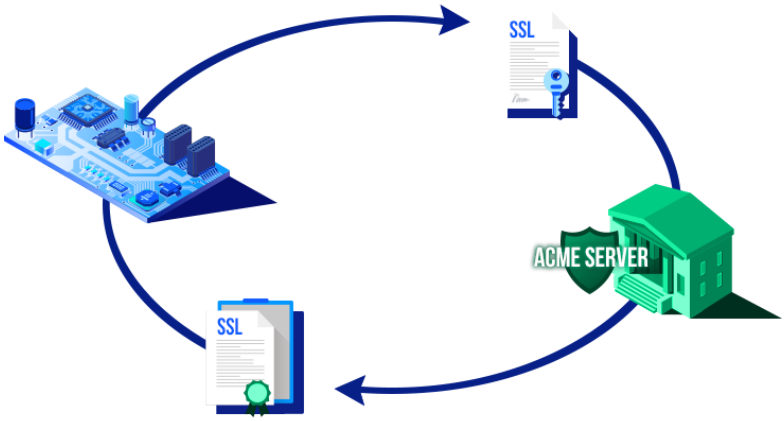
CycloneACME v2.2.4

Embedded ACME Library for MCU

CycloneACME is a client implementation of ACME (Automatic Certificate Management Environment) dedicated to embedded applications. This solution can be used to automate the process of managing X.509 certificates (ordering, renewal, revocation) with a remote certification authority like Let's Encrypt. ACME allows deployment of public-key infrastructure on Internet-facing devices (HTTPS server for example) at 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

© 2010-2023 Oryx Embedded

CycloneACME v2.2.4

Embedded ACME Library for MCU

Supported Processors

- ARM Cortex-M3
- ARM Cortex-M33
- ARM Cortex-M4
- ARM Cortex-M7
- ARM Cortex-R4
- ARM Cortex-A5
- ARM Cortex-A8
- ARM Cortex-A9
- Legacy ARM7TDMI / ARM926EJ-S
- RISC-V
- MIPS M4K
- MIPS microAptiv
- Infineon TriCore AURIX
- PowerPC e200
- Coldfire V2
- RX600
- AVR32
- Xtensa LX6

Supported Compilers / Toolchains

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

Supported Operating Systems

- Amazon FreeRTOS
- ChibiOS/RT
- CMSIS-RTOS
- CMSIS-RTOS2
- CMX-RTX
- Keil RTXv4 and RTXv5
- Micrium µC/OS-II and µC/OS-III
- Microsoft Azure RTOS (ThreadX)
- Segger embOS
- TI-RTOS (SYS/BIOS)
- Zephyr RTOS
- Bare Metal programming (without RTOS)

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

© 2010-2023 Oryx Embedded