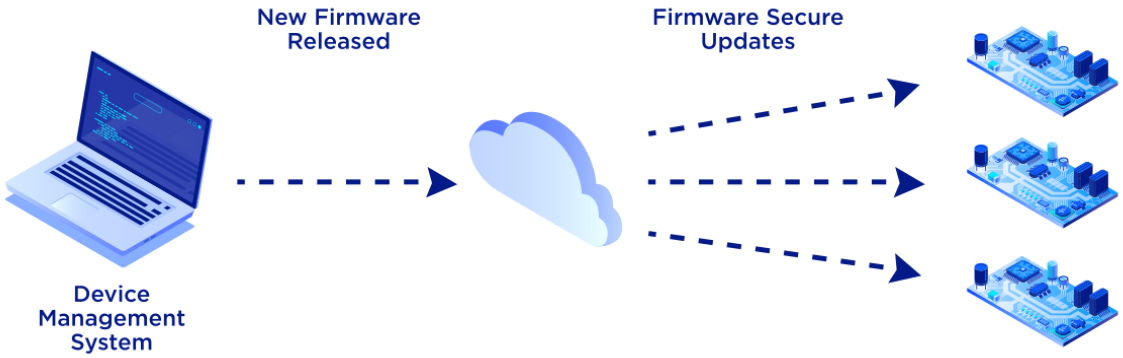
CycloneBOOT

CycloneBOOT is a secure firmware update solution targeting 32-bit microcontrollers. It provides a reliable and secure method for booting and updating the firmware of your device. Tailored to work with a variety of ARM Cortex-M based microcontrollers, CycloneBOOT ensures a seamless boot process every time.



Main Features

CycloneBOOT includes several security measures to protect against external threats and unauthorized access. It features a secure boot process that verifies the integrity of the firmware update before processing it. It is also capable of working with encrypted firmware and supports authentication or digital signature to verify the incoming firmware updates.

CycloneBOOT is protocol agnostic, allowing firmware updates to be performed using various communication channels such as Ethernet, USB, UART, Wi-Fi, Cellular Modem, etc. It features a simple and intuitive interface, making it easy to integrate alongside your existing firmware and your favorite protocol.

CycloneBOOT offers versatile support for various memory partitioning configurations. Featuring In-Application Programming (IAP), it accommodates Single Bank MCUs used with or without external flash, as well as Dual Bank MCUs. This flexibility enables to tailor the boot process to suit different scenarios.

CycloneBOOT includes fallback and anti-rollback support to ensure that your device is always able to boot, even in the event of a failure. The fallback feature allows user to revert to a previous firmware if the latest firmware contains bugs or serious issues. The anti-rollback feature prevents unauthorized downgrades of the current firmware, ensuring that only latest versions of the firmware are used. This helps to protect against potential vulnerabilities that may exist in older firmware versions.

Detailed Feature List

- Secure firmware update solution for 32-bit MCUs (ARM Cortex-M)
- Include an Update Library and a static Bootloader
- Can be integrated in client or server operation
- Support for In-Application Programming (IAP)
- Support for MCU with Dual Bank or Single Bank Flash
- Support for external Flash (on request)
- Can run alongside a RTOS or in Bare Metal
- Support for encrypted firmware image using AES-CBC
- Integrity verification of firmware (CRC32, MD5, SHA-1, SHA-224, SHA-256, SHA-384 or SHA-512)
- Authentication of firmware using HMAC
- Signature of firmware using RSA or ECDSA
- Fallback support (restore previous firmware version if needed)
- Anti-rollback support (prevent installing a previous firmware version)
- CLI tool running on Windows or Linux to build a secure firmware image (can encrypt the firmware and compute an integrity tag, an authentication tag or a signature)

Easy to use with TCP/IP Protocols

With our experience on TCP/IP protocols we can provide you with a ready-to-use Ethernet Bootloader by bundling CycloneBOOT with CycloneTCP (TCP/IP stack), CycloneSSL (TLS library) and CycloneSSH (SSH library). You could for example fetch the new firmware image over Internet (LAN, Wi-Fi, Cellular Modem) using protocols like:

- TFTP / FTP / FTPS
- HTTP / HTTPS
- MQTT / MQTTS
- SFTP / SCP ...

Supported Microcontrollers

- STM32L4
- STM32F4
- STM32F7
- STM32H7
- STM32U5

Supported Toolchains / Compilers

Toolchain / IDE	Compiler
Makefile	GCC
IAR Embedded Workbench	EWARM
Keil MDK-ARM	ARM Compiler v5, ARM Compiler v6 (CLANG)
Segger Embedded Studio	GCC
ST STM32CubeIDE	GCC