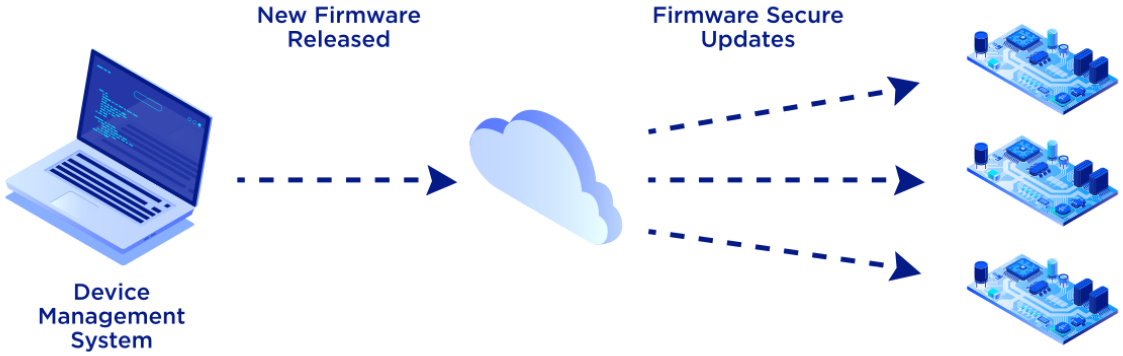
CycloneBOOT

CycloneBOOT is a secure bootloader targeting 32-bit microcontrollers. It is designed to provide a reliable and secure method for booting your device. It is tailored to work with a variety of ARM Cortex-M based microcontrollers, ensuring a seamless boot process every time.



Main Features

CycloneBOOT is equipped with several security features to protect against external threats and unauthorized access. It includes a secure boot process that verifies the authenticity of the firmware image before processing it, ability to work with encrypted firmware update images, as well as support for digital signatures to verify the identity of the image.

In addition to security, CycloneBOOT is designed for ease of use. It is protocol agnostic, meaning that a firmware update can be performed using various physical media (Ethernet LAN, Wi-Fi, Cellular Modem, USB, UART, SD card...). CycloneBOOT features a simple and intuitive interface, allowing you to easily integrate CycloneBOOT alongside your existing firmware. It also includes support for multiple boot configurations — Single Bank with a static bootloader, Dual Bank with "In-Application Programming" where no bootloader is required to update the firmware — allowing you to customize the boot process for different scenarios.

CycloneBOOT is designed with reliability in mind. It 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 image if the latest firmware image contains bugs or serious issues. The anti-rollback feature prevents unauthorized downgrades of the main firmware image, ensuring that only authorized and secure versions of the firmware are used. This helps to protect against potential vulnerabilities that may exist in older firmware versions.

Detailed Feature List

- Secure bootloader for 32-bit microcontroller
- 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
- Integrity verification of the firmware image using CRC32, MD5, SHA-1, SHA-256 or SHA-512
- Authentication of the firmware image using HMAC
- Signature of the firmware image using RSA or ECDSA
- Support for encrypted firmware image using AES-CBC
- Fallback support (Backup current firmware and restore it if required)
- Anti-rollback support (Prevent rolling-back to a known faulty firmware version)
- PC utility running on Windows or Linux to build the firmware image (can encrypt the firmware and compute an integrity tag, an authentication tag or a signature)

Supported Microcontrollers

- STM32L4
- STM32F4
- STM32F7
- STM32H7
- ATSAME54

More to come!

Supported Compilers / Toolchains

- GNU GCC / Makefile
- Atollic TrueSTUDIO
- IAR Embedded Workbench
- Keil MDK-ARM
- SEGGER Embedded Studio
- AC6 System Workbench for STM32 (SW4STM32)
- ST STM32CubeIDE

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 ...