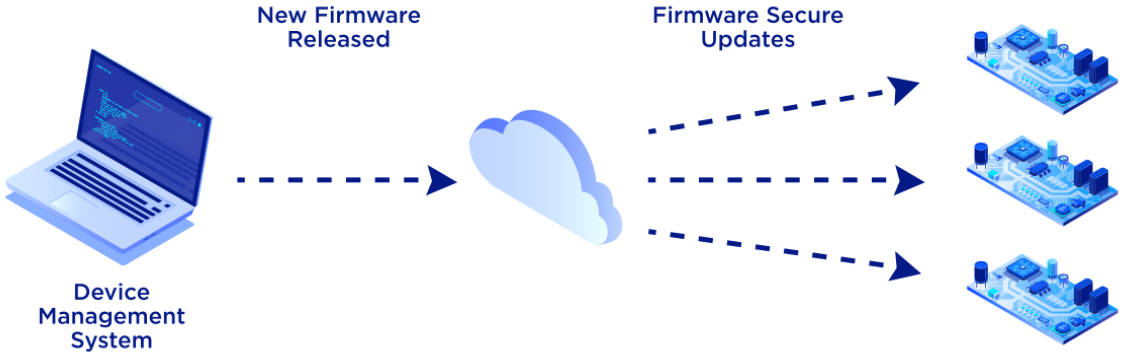
CycloneBOOT

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 an advanced verification process that checks the integrity of firmware update images before processing them. It is also capable of working with encrypted firmware update images, and it supports authentication or digital signature to verify the incoming firmware update images.

CycloneBOOT offers versatile support for various memory partitioning configurations. It accommodates different MCU internal flashes, whether used with or without external flash. It can also enable In-Application Programming (IAP) with dual-bank flash MCUs. This flexibility allows the boot process to be tailored to different scenarios depending on the desired levels of security and reliability.

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.

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.

We can help you compare these features and different update scenarios, and provide a custom demo tailored to your needs (desired scenario, eval board, toolchain). As always with ORYX, you can evaluate the full source code!

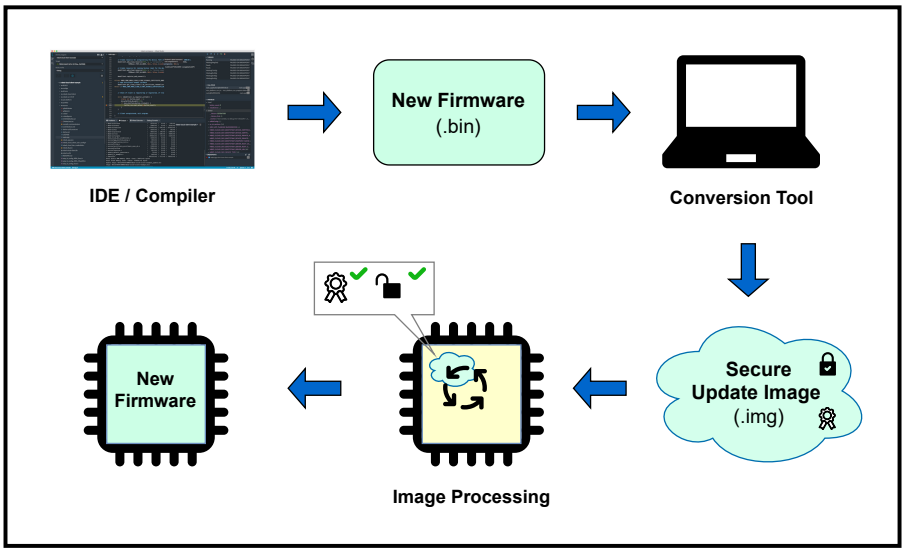
Detailed Feature List

- Secure firmware update solution for 32-bit MCUs (ARM Cortex-M)
- Support for various MCU internal flashes and external flashes
- Support for In-Application Programming (IAP) when using MCUs with dual-bank flash capabilities
- Support for encrypted firmware update images using AES-CBC
- Integrity verification of firmware update images (CRC32, MD5, SHA-1, SHA-2)
- Authentication of firmware update images using HMAC
- Signature of firmware update images using RSA or ECDSA
- Fallback support (restores previous firmware version if needed)
- Anti-rollback support (prevents installing a previous firmware version)
- Can be integrated in client or server operation
- Can run alongside a RTOS or in Bare Metal

Modular Functionalities

CycloneBOOT solution provides modular functionalities that can be enabled separately or integrated together, depending on the desired update scenario:

- An **update library**, integrated within your user application, for processing incoming firmware update images.
- A **multi-stage bootloader** (optional immutable first-stage bootloader to enable updatability of the second stage) supporting advanced features such as firmware verification at every startup, fallback mechanisms, and management of external flash.
- A **standalone bootloader** managing the entire firmware update process, including reception, validation, and installation. In this case, the bootloader includes a predefined protocol.
- A **CLI tool (ImageBuilder)** running on Windows or Linux to build secure firmware update images. It 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
- STM32H5
- ATSAME54

Supported Toolchains / Compilers

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