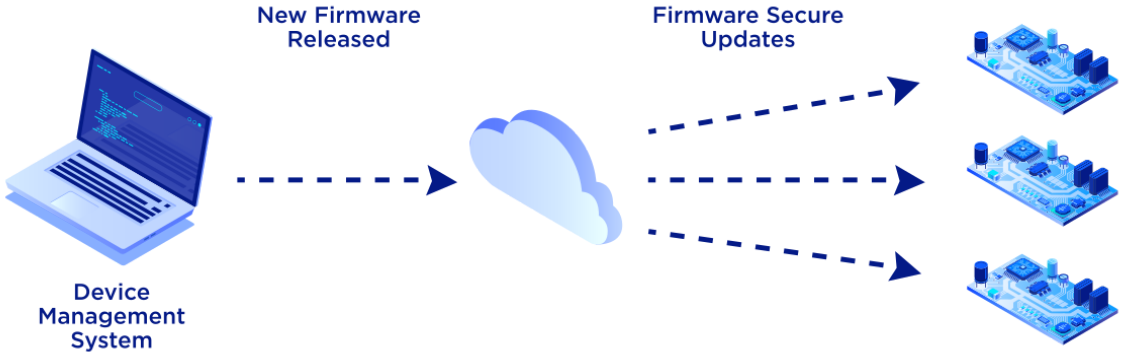
CycloneBOOT

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 multiple security measures to protect against external threats and unauthorized access. It features an advanced verification process that can be enabled to check the integrity of firmware update images before processing. It can also handle encrypted firmware update images and optionally supports authentication or digital signatures to verify incoming updates. Additionally, boot-time application firmware verification using RSA or ECDSA signatures for Secure Boot can be activated as needed.

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.

Detailed Feature List

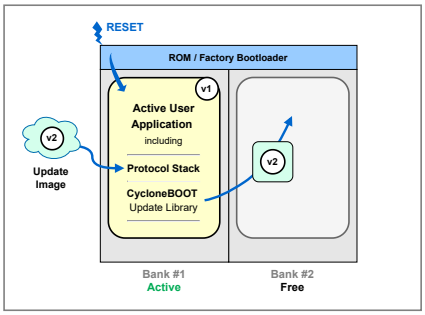
- Secure firmware update solution for 32-bit MCUs (ARM Cortex-M)
- Support for various MCU internal flashes and external flashes
- Support for In-Application Programming (IAP) when using MCUs with dual-bank flash capabilities
- Update image verification using MD5/CRC32/SHA-1/SHA-2 integrity checks, HMAC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

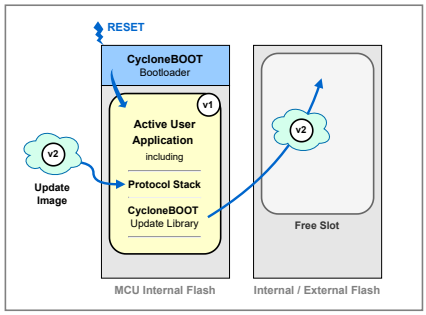
Modular Architecture

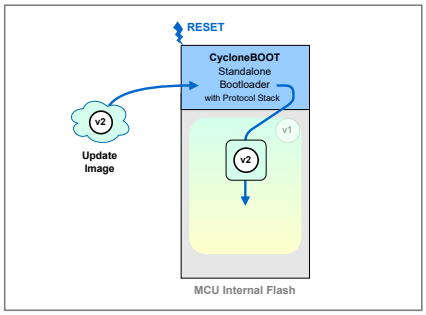
CycloneBOOT solution provides modular architecture whose components can be enabled independently or integrated together, depending on the desired update scenario:

- **CycloneBOOT Update Library** integrated within the user application, can process incoming update images, including reception, validation, and installation or storage. It can also enforce anti-rollback protection.
- **CycloneBOOT Bootloader** can install update images and supports advanced features such as application firmware verification at every startup (Secure Boot), fallback mechanisms, and external flash management. The optional multi-stage approach provides an immutable first-stage bootloader that enables the second stage to be updated.
- **CycloneBOOT Standalone Bootloader** manages the entire firmware update process, including reception, validation, and installation. In this case, the bootloader also includes a predefined protocol.

We can help you compare these features and various update scenarios, and provide a custom demo tailored to your needs. As always with ORYX, the full source code is available for evaluation!

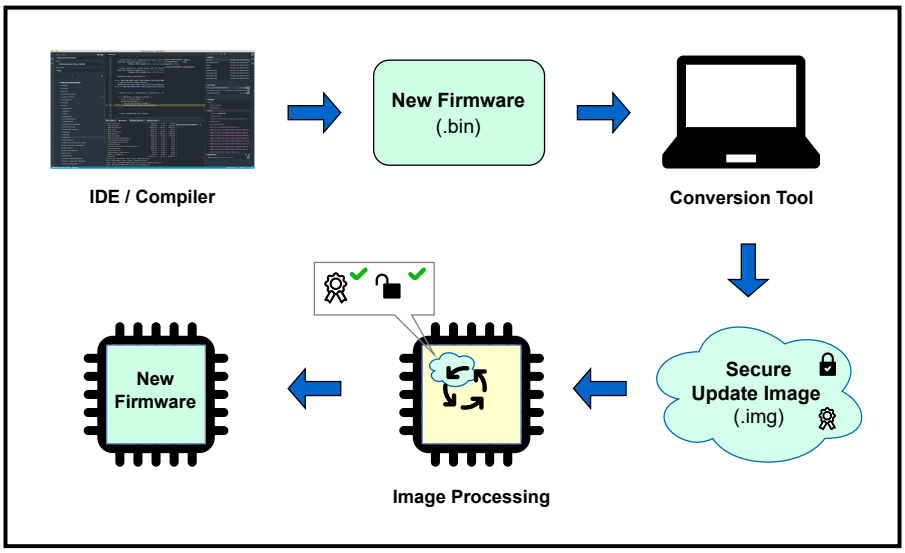






ImageBuilder Tool

ImageBuilder is a cross-platform CLI utility (Windows and Linux) for building secure firmware update images, with support for encryption, integrity tags, authentication tags, and signatures. It can also generate signature keys.



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