Cypherbridge® Systems
uLoadXL Secure Boot & Installer
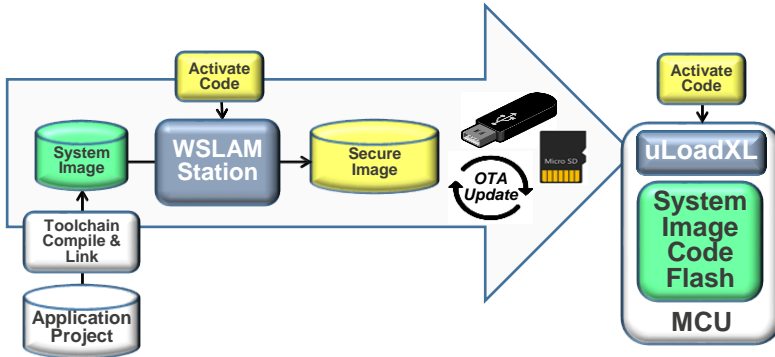
Cypherbridge®
Trusted, safe and secure

Overview

The uLoadXL SDK delivers advanced secure boot loader and software update solutions for embedded platforms. uloadXL can manage software updates and distribution, encrypt images, authenticate genuine origin, and block malware.

The WSLAM Windows GUI signs and encrypts the system image using key material and user supplied private activation code. Secure managed images can be transferred by email, flash drive, serial port or OTA LAN/WAN network.
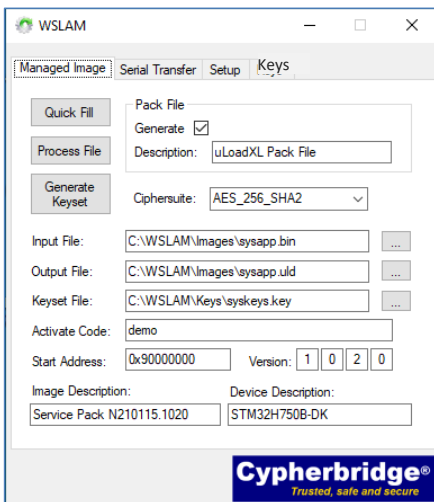
To install the software update on the embedded platform, the activation code is supplied to the loader interactively or under machine control.

The installer decrypts and authenticates the system image and saves it to the target program flash.

An incorrect activation code or a malware image, is blocked from installing and executing.

At power up or reset uLoadXL executes system integrity checks, verifying application signature with configurable fallback and recovery steps.

- ✓ **Platform Kit**. uLoadXL APIs are interfaced to the embedded target via integrated Platform Kit including standalone drivers for internal MCU flash, external QSPI flash, removable media and serial I/O channels.

- ✓ **Multiple Images.** The uLoadXL embedded system and APIs can manage multiple images. Workflow can be programmed to install, save and activate A/B image firmware and auxiliary files.

- ✓ **Registry.** Loader maintains image registry information including status and authentication signatures. System application is verified before starting execution to detect corrupt image or malware intrusion attempt.

- ✓ **Security Model.** uLoadXL implements an advanced key system, selectable cipher suite, code sign and verify and protected embedded key material container, with anti-rollback protection.

- ✓ **Robust.** System integrity, safety and availability features include primary and backup registry copies, power fail recovery, primary and recovery image, and failsafe options.

Features

- ✓ *Add product integrity, block hacking and malware, control optional feature distribution*

- ✓ *Secure boot root of trust*

- ✓ *Install software updates for system application, graphic menus, FPGA bit files*

- ✓ *Image file encryption, integrity and authentication, code sign and verify. Image cannot be hacked if lost or intercepted*

- ✓ *Install from serial port, file system, Over the Air Update*

- ✓ *Integrated loader verifies system application integrity, rollback to recovery image, & executes failsafe boot*

- ✓ *Use standard toolchain to compile and link application system image*

- ✓ *Windows WSLAM Software Management Station GUI*

- ✓ *LCD graphic progress messages and progress bar display framework*

- ✓ *NIST 800-193 Firmware Protect, Detect and Recover*

- ✓ *Platform Kits available for off the shelf MCU evaluation kits*

- ✓ *Customizable for OEM product design*