Cypherbridge® Systems uLoad™ Install Defender ™ Edition

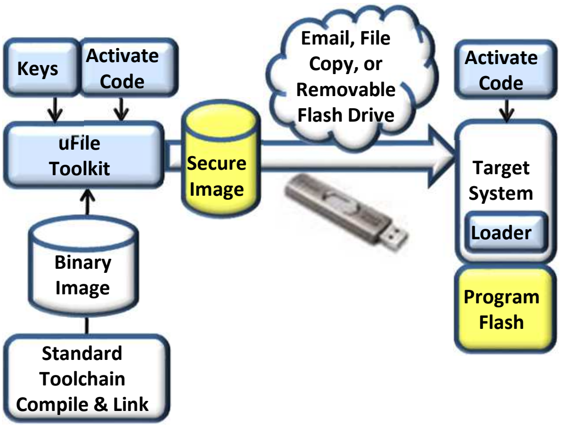
Cypherbridge Systems

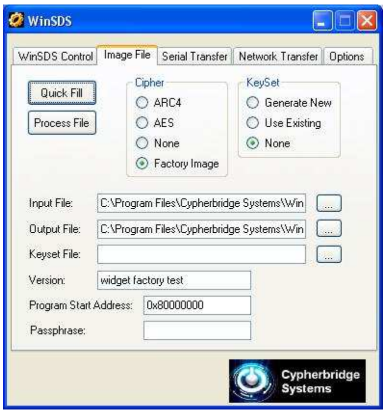
Overview

The uLoad SDK product family delivers advanced software update and boot loader solutions for embedded platforms. The uLoad Install Defender Edition controls software updates and distribution, authenticates genuine origin, and blocks malware installs.

uLoad IDE includes a command line toolkit or Windows GUI for image encryption using multi-level keys and activation code

Secure images can be transferred by email, file copy, local USB or SD flash drives, serial port or LAN/WAN network.




WinSDS

WinSDS Control | Image File | Serial Transfer | Network Transfer | Options

Quick Fill

Process File

Cipher: ○ ARC4 ○ AES ○ None ● Factory Image

KeySet: ○ Generate New ○ Use Existing ● None

Input File: C:\Program Files\Cypherbridge Systems\Win ...

Output File: C:\Program Files\Cypherbridge Systems\Win ...

Keyset File: ...

Version: widget factory test

Program Start Address: 0x80000000

Passphrase:

Cypherbridge Systems

When a software update is started on the embedded platform, the activation code is supplied to the install defender loader, interactively by a field engineer or user, or securely stored in target.

The Install Defender loader authenticates the system image, decrypts it, and saves it to the target program flash.

An incorrect activation code, or a rogue image, is blocked from installing to prevent unauthorized use, malware hack, or reverse engineering

The uLoad Product Family includes advanced software update and boot loader solutions for embedded platforms. uLoad can be used for safe install, manage multiple images to update, activate and safe-boot to last-known-good or factory version, and integrate a boot loader with optional security features:

✓***uLoad-IDE*** Install Defender controls software updates and distribution, authenticates genuine origin, and blocks malware in SCADA, POS terminals, industrial controllers, and anytime software updates are used.

✓***uLoad-DFE*** Device Firmware Edition manages multiple factory and clear text images with zero encryption or passphrase. It is targeted for embedded systems to manage multiple images and rollback features in a robust solution. Images are managed the same way as the uLoad Secure Edition, only without encryption.

✓***uLoad-SE*** Secure Edition manages multiple encrypted images and multi-level keys. Images can be authenticated and decrypted during the installation, or during the boot loading stage, to defend against hacking and reverse engineering, and control optional software feature distribution.

Features

- ✓ *Adds product Integrity, block hacking & malware, and control optional feature distribution*
- ✓ *Install software updates for executable images, graphic menus, FPGA bitstream files*
- ✓ *Adds file encryption, hash integrity and authentication*
- ✓ *SD or USB file system included*
- ✓ *Loader includes INI script, fallback recovery image, and failsafe boot to system application*
- ✓ *Use standard toolchain to compile and link software image. Supports IAR, Keil, GCC and all other toolchains*
- ✓ *uFile image toolkit supported on command line, Windows GUI, and MacOSX*
- ✓ *Email or transfer files encrypted files safely*
- ✓ *Image cannot be hacked if USB flash drive or embedded system is lost or stolen*
- ✓ *Loader integrated as low footprint target application*
- ✓ *Install can be integrated in system GUI and cmd shell*

For Pricing and Availability

Cypherbridge Systems, LLC
7040 Avenida Encinas #104211
Carlsbad CA 92011 USA +1 (760) 814-1575
www.cypherbridge.com
sales@cypherbridge.com

CSL-uLoad-IDE-140814.1

Features and specifications subject to change without notice