

# Cypherbridge® Systems

## uLoad Secure Boot Loader and Installer

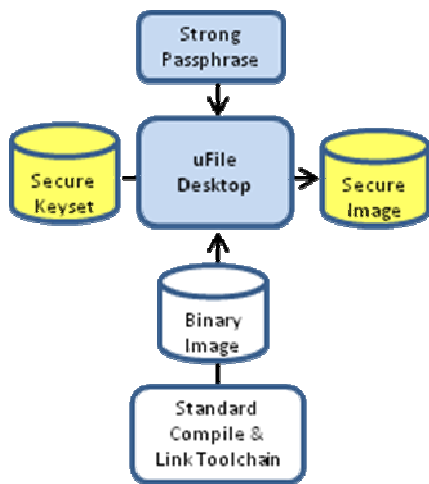


### Overview

uLoad is a secure installer and boot loader SDK designed for embedded platforms. uLoad can manage multiple images to install, activate and rollback to last-known-good. It utilizes standards based commercial grade security to generate a compact security header with hash signature and file encryption to secure the image file.

Secure firmware image files are authenticated during MCU installation using the security header. Multiple firmware images can be managed on-chip or on-board. Once the image is authenticated, key information is extracted from the image security header and used to decrypt the firmware image. uLoad also provides version upgrade and rollback features for firmware field upgrades and product support.

Figure 1: uFile Image Process



### uFile Image Process

With no change to existing tool chains, binary firmware or FPGA images are processed by the uFile command tool. This generates keysets and adds the security header to the binary image. The header includes versioning, digital signature, and security fields to protect the target platform from un-authorized images or reverse engineering attacks.

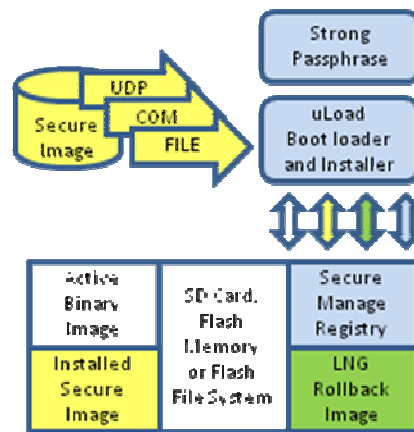
The multi-layer key system scrambles the firmware decryption key with a master key so the decrypt key can be embedded in the firmware image header and safely distributed inside the secure image. Generated keys sets are protected by a strong passphrase, so keys are protected at-rest or even emailed independently of firmware images. Finally, the master key associated with the firmware image is used to activate the decryption key at the manufacturing line or in the field. uLoad multi-key encryption insures that the master key can only be activated with the passphrase supplied during image preparation.

### Boot loader and Installer

The MCU executes the boot loader early in the firmware start cycle. A security check verifies the active firmware image signature before executing the active image application code.

The installer can be used from interactive login or called from application code for image file maintenance, installation, upgrade and rollback. Local and remote secure image source and destination endpoints are supported

Figure 2: Boot and Install



uLoad is available on a range of platforms including CM3, and integrated with leading RTOS and tools including IAR and GCC.

### Features

- ✓ Enhance product integrity, block reverse engineering, and control firmware option distribution.
- ✓ Image file hash authentication and encryption
- ✓ Serial port interface, removable and fixed flash file systems for file load and save
- ✓ Easy to use session initialization with flexible source and destination endpoints for secure image files and keysets
- ✓ Managed registry retains image history for install, active and rollback images across power cycles.
- ✓ Powerfail recovery and registry rebuild
- ✓ uFile desktop keyset generator and image file processor available for Windows and Linux
- ✓ Portable ANSI-C small RAM and ROM footprint with royalty-free source code license

### Options

- ✓ Multipoint remote install over IP network
- ✓ uFile APIs for integration with device management system
- ✓ DS28E01 trust chip driver and MCU/FPGA interface security engine

### For Pricing and Availability Contact:

Cypherbridge Systems, LLC  
 7040 Avenida Encinas #104211 Carlsbad, CA 92011  
 www.cypherbridge.com  
 sales@cypherbridge.com  
 Tel: (760) 840-0629

### About Cypherbridge Systems:

Established in 2005 to offer software, server, security, device and system level products, our portfolio includes software stacks to enable a broad range of connected device applications integrating embedded device, communications networks, and back office servers in a system solution.

Copyright © 2010 Cypherbridge Systems, LLC.

Product features and specifications subject to change without notice.

CSL-0630.1