

Mocana CyberBoot™

Multi-stage, multi-key verification of boot loaders and boot images for UEFI-based boot sequence on Linux platforms

The Mocana® CyberBoot™ Client provides multi-factor verification of the UEFI-based boot sequence on Linux platforms and tamper-resistant updates of signing keys, boot loaders, and boot images with supply chain integrity.

The CyberBoot Client is comprised of the following components:

- › Mocana-issued public key (in the UEFI key store)
- › Mocana secondary boot loader (MSBL)
- › Mocana CyberBoot loader (MCBL)
- › Scripts to pull, sign, and push images from and to the target device

How It Works

Figure 1 below describes the Mocana CyberBoot verification process and client components:

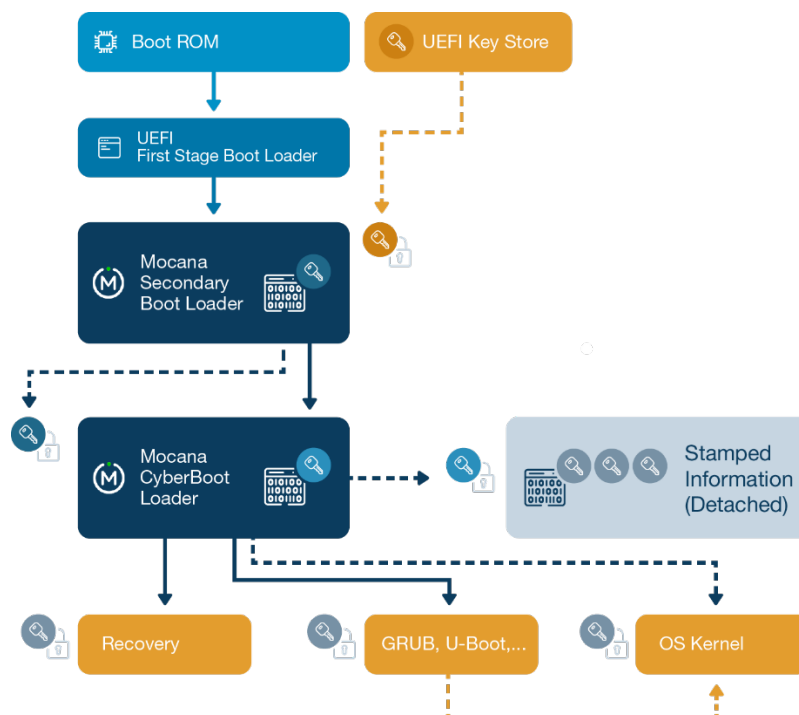


Figure 1. Mocana CyberBoot Client Components

Features and Benefits

- › Small code and runtime footprints
- › FIPS-validated cryptographic algorithms
- › Secure pre-boot verification of boot loaders and images
- › Prevents boot sequence code tampering
- › Blocks unlicensed upgrades
- › Guaranteed GPL-free code protects your intellectual property
- › Zero-coding, plug-and-play solution
- › Integrated with TrustCenter for tamper-resistant updates with supply chain integrity

About Mocana

Mocana protects more than 100 million devices worldwide and is trusted by the largest aerospace, industrial, energy, healthcare, and communications companies. Find out more at www.mocana.com.

Mocana Corporation

1735 N First Street, Suite 306

San Jose, CA 95112

tel (415) 617-0055 toll free (866) 213-1273

sales@mocana.com