Aptio V UEFI Firmware Deep Dive

MOVING BEYOND LEGACY BIOS
WITH A MODERN UEFI SOLUTION

REVISION 1.8.1 – APRIL 15, 2021

Aptio V UEFI Firmware Deep Dive

04/15/2021

Revision History

2013-01-03	1.30	First release for internal review
2013-01-16	1.31	Edits made from internal review
2013-07-09	1.40	Updated for current status of Aptio® V
2014-06-30	1.41	Updated Utility OS support information
2014-09-16	1.42	Edits made from internal review
2015-03-26	1.43	Edits made from internal review
2015-07-28	1.44	Updated Features
2015-11-24	1.45	Updated Features
2016-02-10	1.46	Updated Features
2017-11-15	1.5	Updated and Added Features
2018-01-03	1.6	Updated feature information and specification versions
2021-03-12	1.7	Updated feature information and specification versions
2021-04-09	1.8	Updated document template
2021-04-15	1.8.1	Updated type of document to Deep Dive

Disclaimer

Although efforts have been made to assure the accuracy of the information contained here, AMI expressly disclaims liability for any error in this information, and for damages, whether direct, indirect, special, exemplary, consequential or otherwise, that may result from such error, including but not limited to the loss of profits resulting from the use or misuse of the User Guide or information contained therein (even if AMI has been advised of the possibility of such damages). Any questions or comments regarding this User Guide or its contents should be addressed to AMI at the address shown on the inside of the front cover.

AMI provides this publication "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability or fitness for a specific purpose.

Some states do not allow disclaimer of express or implied warranties or the limitation or exclusion of liability for indirect, special, exemplary, incidental or consequential damages in certain transactions; therefore, this statement may not apply to you. Also, you may have other rights that vary from jurisdiction to jurisdiction.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. AMI may make improvements and/or revisions in the product(s) and/or the program(s) described in this publication at any time.

Requests for technical information about AMI products should be made to your AMI authorized reseller or marketing representative.

Table of Contents

Chapter 1 Introduction

Purpose of this document

AMI presents Aptio® V as the next-generation solution for UEFI BIOS. Aptio® V incorporates over 25 years of experience delivering AMIBIOS solutions while moving beyond legacy BIOS limitations. Aptio® V is a highly modular solution, portable across a variety of platforms. The Aptio® driver model, based on Unified EFI (UEFI) and the Intel® Platform Innovation Framework for UEFI, delivers higher flexibility than legacy BIOS and provides new opportunities for applications in the pre-boot environment.

Aptio® V Key Features

- UEFI & Intel Platform Innovation Framework for UEFI
  - Supports Integration with Intel EFI Development Kit (EDK2) and “Tiano” drivers
  - Support for UEFI 2.8 and PI 1.7
  - Support for x86/x64 and ARM processors
  - Support for Windows® and Linux build environments
  - Microsoft® Windows® 8/8.1/10 support
  - NIST SP 800-147 BIOS Protection Guideline compliance (Secure Flash)
- A Single UEFI Core for all market segments
  - Desktop, Mobile, Server, Embedded and Tablets
  - Core is validated across multiple PC market segments
- Supports Multiple Silicon Vendors
  - Wide Range of CPUs and chipsets supported
    - Available for both Intel®, AMD, VIA and ARM AArch64 reference platforms
- A Complete UEFI Solution
  - Codebase optimized for size and boot time
  - Template-based chipsets deliver a consistent development experience despite differences in platforms
  - BIOS setup touch screen support
  - Development and Debug Tools
    - Visual eBIOS (VeB) Development Environment
    - AMI Debug for UEFI
  - Deployment Utilities:
    - Flash utilities for multiple operating systems
    - AMIBCP, MMTool, and ChangeLogo for ROM image maintenance
    - DMIEDIT for SMIBIOS configuration during manufacturing
    - AMISLP for adding the Microsoft System Locked Pre-Installation keys into the BIOS to support OEM activations of Microsoft® Windows®
- Smooth Migration from legacy BIOS to UEFI with Aptio® V
  - A full Compatibility Support Module (CSM), based on AMIBIOS8, which adds legacy BIOS interfaces to Aptio® for non-UEFI OSes – support is reliant upon hardware compatibility

- The Visual eBIOS (VeB) Development environment offers a common environment for working with both AMIBIOS8® and Aptio®
- AMI offers worldwide engineering support; cross-trained for AMIBIOS8® and Aptio® solutions

Chapter 2 UEFI Background

What is UEFI?

The Unified Extensible Firmware Interface (UEFI) specification defines a modern API for operating systems to interface with platform firmware. The interface consists of data tables filled with platform specific information, plus boot and runtime functions that are available to the operating system and its loader. Together, these interfaces provide a standardized environment for booting to operating systems and for executing pre-boot applications.

For more information on UEFI, visit https://www.uefi.org.

How Does UEFI Relate To BIOS

UEFI standardizes two primary functions of the PC Basic Input/Output System (BIOS): creating a standard firmware-to-OS interface and performing initialization of the platform's hardware. The UEFI Specification Work Group (USWG) releases the UEFI specification, which describing the firmware-to-OS interface. The Platform Initialization Working Group (PIWG) releases a Platform Initialization specification, which describes a standardized way to implement the platform initialization. The purpose of these two specifications is to promote interoperability between the firmware of both platforms and silicon vendors by providing a standard set of functionality independent of the platforms.

A Brief History of BIOS

The Basic Input-Output System (BIOS) of the original IBM PC/XT and PC/AT, while being a very small part of the entire system package, was the key to the success of the PC architecture. The clean definition of the PC/AT BIOS gave companies the ability to create "clone" the original systems. These clones quickly dominated the budding PC market. The wide spread availability of MS-DOS allowed applications to run the same across different brands of beige-box "PC clones". As more companies entered the PC market, basic economics took over and prices decreased. Because of the firmware interfaces IBM designed for the original 250,000 IBM PC/XT systems, a firmware industry blossomed to support the PC market.

While BIOS are independent of the Operating System, they are very platform specific. At the heart of the BIOS is the Intel® 8086 processor, which is based upon Intel's software interrupt model. This model's underpinnings have always been backward compatible, which means the current generation of x86/x64 processors would still boot to an operating system via the original IBM PC/XT method, in Intel's 8086 "real mode".

From BIOS to UEFI

The need for systems to be compatible with the BIOS interface dictate how processor companies, like Intel®, design their processors and chipsets. The problems with this process became apparent to Intel® when they were developing the 64-bit Itanium architecture. EFI was created as a way to separate the processor architecture from the OS-to-firmware interface. After EFI was used on Intel® Itanium products, EFI was migrated into the x86 architecture.

UEFI is the successor to the Intel® Extensible Firmware Interface (EFI). The UEFI Forum, a collaborative, non-profit corporation, was formed to promote and manage the UEFI specifications. AMI is a UEFI Promoter and on the board of directors.

The Intel® Platform Innovation Framework for EFI

The Intel® Platform Innovation Framework for EFI (also known as “the Framework”) was the original set of specifications developed by Intel® to describe an EFI environment. The Framework specifications described the OS-to-firmware interfaces, as well as structures and functions available to the firmware for the platform specific initialization. The Framework specifications have since been eclipsed by the Platform Initialization specification and the UEFI specification.

Platform Initialization (PI)

While the UEFI Specification defines the interface between the operating system and the system firmware, the Platform Initialization (PI) specifications describe how the system firmware is constructed to perform the platform specific hardware initialization. The PI specification builds upon the concepts designated in the Framework and formalizes these concepts into an industry supported specification. Firmware vendors who follow the PI specification can easily add 3rd party developed code to their projects. Aptio® V supports the PI 1.7 specification, which includes numerous security improvements.

Aptio® V Support for UEFI

The Aptio® V core architecture supports the UEFI 2.8 specifications, introducing new security concepts intended to improve platform security.

AMI’s Work with UEFI

As an early adopter of EFI, and founding member of the UEFI Forum, AMI sees UEFI as an evolution of the original BIOS. AMIBIOS8® introduced modern firmware development methods, such as graphical development tools and modular components, but the final interfaces produced by the BIOS were restricted by the necessity of backward compatibility for the original BIOS interfaces. AMI leveraged the ideas introduced in the UEFI specification to create Aptio®, which provides new opportunities for firmware developers.

The UEFI model allows AMI engineers to focus on feature support and less on compatibility issues, such as support for booting from USB devices. A legacy OS-loader with no native support for USB devices would have relied on the legacy BIOS INT 13h interface, which would emulate USB devices as floppy disks or hard disks. For the INT 13h interface to support the myriad of USB storage devices, AMI engineers previously had to focus on supporting legacy emulation of the USB devices instead of developing new features.

With UEFI, product features can be ported cross-platform using a new platform independent model. Moving away from the 16-bit BIOS model of the 1980's has allowed UEFI firmware products like Aptio® to move the market forward.

(Intentionally Blank)

Chapter 3 Major Features of Aptio® V

Standards Based Development

Through the support of UEFI, Aptio® V offers developers a clean implementation based on the latest firmware standards. Aptio® V supports UEFI IA32, x64, and ARM architectures; as well as support for directly integrating EDK II drivers.

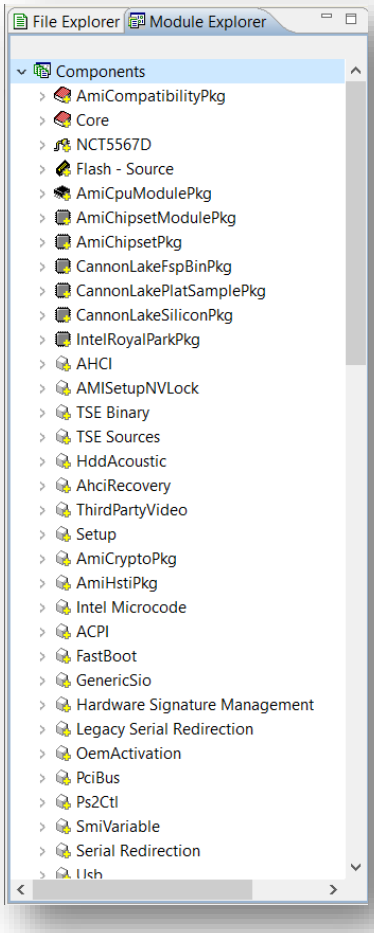
Single UEFI Core for Any Application

Aptio® relies on the same philosophy that made the AMIBIOS8® successful: "one core for any application." The modular Aptio® architecture allows the same stable core to be deployed for Desktop, Mobile, Server, Embedded, Tablet and Ultra Mobile (UMPC) projects. Aptio® V offers a validated UEFI solution for use in multiple PC market segments and through various vertical markets.

The "one core" approach is why Aptio® is available on a variety of Intel® Customer Reference Board (CRB) platforms from the Mobile Platform Group (MPG), Embedded and Communications Group (ECG) and Ultra Mobile Group (UMG).

Supports Multiple Silicon Vendors

Aptio® is based on a combination of the EDK II development environment plus AMI's additional components, which allows for easy porting to any vendor's CPU or chipset. Aptio® has already been ported to a broad set of CPU and chipsets, including offerings from Intel, AMD and ARM.



Modular Core Design

By leveraging AMI's Component Information Format (CIF) and System Description Language (SDL) technologies, Aptio® developers have combined UEFI concepts with AMI's eModule design. Platform specific changes are separated from the hardware initialization modules. Customers can leverage the modularity to quickly port OEM customizations from one platform to the next.

Complete UEFI Solution

Aptio® V is offered as a complete UEFI solution. This solution includes an optimized codebase, development tools, deployment utilities, training programs and worldwide engineering support. The Aptio® V solution provides all of the pieces customers need to solve the puzzle of migrating platforms from a legacy BIOS to a UEFI environment.

Superior Development Tools

As with AMIBIOS8® and Aptio® 4.x, Aptio® V uses the Visual eBIOS (VeB) development environment. VeB is built specifically for firmware development and firmware porting. The latest version of VeB is built on top of the Eclipse development environment. Section 4 of this document describes the many advantages VeB offers to Aptio® developers.

Template Based Porting

AMI uses a "template-based porting" methodology with AMIBIOS8® and Aptio® to deliver a consistent development experience independent of the target silicon. This has been carried forward into Aptio® V to allow customers to easily isolate platform specific changes from the generic chipset and core code.

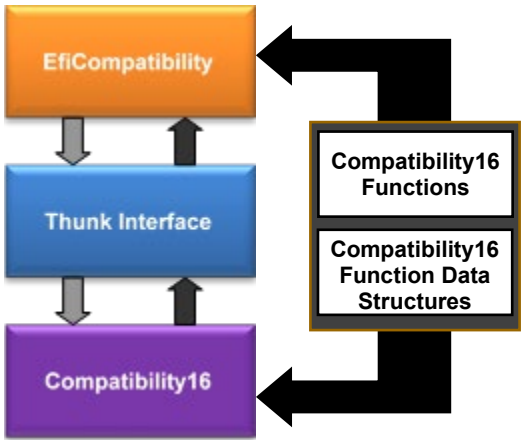
Compatibility Support Module (CSM)

The UEFI specification does not require the legacy BIOS interfaces in the firmware; instead, they leave the legacy BIOS interfaces as an optional portion of the system firmware. Aptio® V still supports these interfaces, thus allowing systems to continue to support non-UEFI operating systems. The interfaces that are still supported include:

- The Legacy Interrupt Interface (INT XXh)

- The BIOS Data Area (BDA) and the Extended BIOS Data Area (EBDA)
- Support for the BIOS Boot Specification (BBS)
- Pointers to firmware data used by legacy operating systems (SMBIOS, ACPI, etc.)
- Support for executing legacy Option ROMs for on-board and add-on devices
- Support for booting to Master Boot Record (MBR) Operating Systems

Some OSes still require legacy support. To meet the requirements of these OSes, AMI has a Compatibility Support Module (CSM) which seamlessly adds support for legacy BIOS interfaces in addition to the UEFI interfaces. This gives customers the flexibility of running newer UEFI-compliant software in addition to legacy Operating Systems, such as MS-DOS, some Microsoft® Windows® systems, Linux and other RTOS environments.



Like other Aptio® components, the CSM is self-contained and can easily be removed from a project. Projects that have no legacy requirements do not need to add the CSM eModule. Projects using the CSM can support both UEFI and legacy Operating Systems while migrating away from legacy BIOS design.

AMI's CSM is based on AMIBIOS8® for maximum compatibility with existing software. The standalone CSM16 (16-bit binary) module requires no addition on top of the standalone binary without the need to make changes to the existing CSM16 binary. These changes are added through porting hooks in the CSM module.

*CSM support is reliant upon hardware compatibility. Some Si vendors may choose not to enable legacy support.

Transitional Support for BIOS Customers

Customers moving their platforms from legacy BIOS or Aptio® 4.x to Aptio® V will find a number of product features designed specifically for a smooth transition.

- Visual eBIOS (VeB): Used by AMIBIOS8® and Aptio
  - Existing AMIBIOS8® customers have no need to learn a new porting tool
  - New AMI customers start using UEFI with a purpose-built development environment
- Compatibility Support Module (CSM)
  - Allows a UEFI firmware based system to boot to a legacy Operating System
  - Based on AMIBIOS8® for maximum compatibility
  - Easily removed if not required
  - *CSM support is reliant upon hardware compatibility
- AMI Worldwide Engineering Support
  - Engineers transfer years of experience in BIOS porting to UEFI designs
  - Support for a wide variety of silicon

- Training is available now
  - For more information on AMI training programs for Aptio see the Aptio Training Data Sheet

Scalable Solution Using eModules and UEFI Drivers

The Aptio® modular design concept allows a project to span across multiple market segments. Customers are no longer locked into the feature sets of a traditional desktop, mobile or server; with Aptio® V, they can pick and choose the exact features they want in their firmware.

A prime example of Aptio® V's flexibility is the fast boot solution. The Fast Boot eModule provides for significantly reduced boot times due to our modular design and based on static configuration.

Microsoft® Windows® 10 Support

Aptio® V offers full Windows® 10 logo compliance. This means support for systems with touch screen capabilities, graphics user interfaces and support for UEFI Secure Boot, in addition to other logo requirements.

Features

Aptio® V features include, but are not limited to, the following:

- UEFI 2.8 Compliance
- PI 1.7 Compliance
- ACPI 6.3 Compliance
- PCI Express 3.1a Compliance
- SMBIOS 3.1.1 Compliance
- UEFI Secure Boot
- NIST 800-147 BIOS Protection Guideline Compliance (Secure Flash update)
- NIST 800-155 Authenticated Firmware
- NTFS file system support
- FAT/exFAT file system support
- ISO9660 file system support
- UDF file system support
- EXT read-only file system support
- Built in UEFI Shell
- Mouse/Touch support
- Soft keyboard support (virtual keyboard)
- Firmware Management Protocol (FMP) support
- ATAPI PassThru protocol support
- iSCSI support (IP based network storage standard)
- IPv4/IPv6 UEFI network support
- Reliability, availability and serviceability (RAS) support
- Runtime error logging support
- USB 1.x, 2.0, 3.x Support
- TPM 1.2 and 2.0 support
- Graphical setup support
- NFC device support
- UEFI 2.5 Smart Card support
- Recovery from EXT file systems
- Recovery from NTFS file systems
- Recovery from FAT/exFAT file systems
- Recovery from ISO9660 file systems
- Recovery from SDIO/MMC devices
- Recovery from USB devices (USB 1.x, 2.0 and 3.x)
- Recovery from Hard Drive devices

- Recovery from CDROM devices
- Recovery via UART
- Opal drive support
- IDE support
- AHCI support
- UFS support
- NVMe boot support
- NVMe SATA password support
- NVMe recovery
- NVMe legacy boot support
- NVMe PassThru protocol support
- PS/2 support
- USB Legacy Emulation support
- FastBoot support
- SMART HDD support
- HDD security support
- Low Power Mode (LPM) Technology
- Intel® vPro Technology (Intel® AMT, Intel® Virtualization Technology (VT-d)
- Intel® Trusted Execution Technology (Intel® TXT)
- Intel® Anti-Theft Technology
- Intel® Thunderbolt Technology
- Intel® Dynamic Power Performance Management (DPPM)
- Intel® Rapid Start technology (Intel® Fast Flash Standby)
- Intel® Smart Connect Technology (Always on Always Connected)
- Fault Tolerant NVRAM support
- Fault Tolerant Recovery support
- Fixed PCI resources support
- UEFI capsule support
- EFI System Resource Table (ESRT) support
- Hidden partition support
- DASH technologies support
- Fixed boot order support
- Computrace Anti-Theft Technology support
- Early video support to display errors and boot progress for select video controllers
- USB Video Class (UVC) support
- Latest IPMI 2.0 support
- PLDM support
- MCTP support
- EBC support
- HSTI support
- Windows OA 1.x/2.x/3.x support
- USB Device Firmware Upgrade support
- Bluetooth and NFC device support
- Intel® Memory Failure Prediction (Intel® MFP) technology support
- DASH-enabled LAN card support
- QEMU-based UEFI firmware emulator
- EXT filesystem driver support
- QR/barcode encoded setup information for manufacturing
- Redfish support (1.8.0)
- Smart update to maintain golden state and reduce possibility of RMA
- Boot performance analysis tool
- Preserve/map NVRAM variables
- Media sanitization support
- Memtest tools

(Intentionally Blank)

Chapter 4 Aptio® V Development Environment

Visual eBIOS Development Environment (VeB)

Aptio® V projects use an updated Visual eBIOS (VeB), with the same look and feel as the one utilized by AMIBIOS8®. VeB is a comprehensive tool that is used during all aspects of platform development.

Project Management

VeB includes tools that allow an engineer to quickly define a new project and include components from a global component. VeB provides a new project wizard that assists the engineer in pulling together components needed to form the project, whether it's based on a reference project, or built from scratch. Once a project has been created, additional components may be added or removed at any time.

Source Control

VeB contains source control integrated tools, with support for multiple formats:

- Git
- SVN
- AMI Remote Source Control (RSC)
- AMI's SVN solution
- AMI's SVN mirroring solution
- Visual Source Safe
- ClearCase
- PVCS
- Dimensions

All standard source control operations can be performed from inside VeB, including check out, check in, get latest, add, remove, show history and difference. Integrating these operations into VeB provides a more convenient way to manage source.

Cross Platform Support

VeB is a cross-platform integrated development environment (IDE) allowing developers the flexibility to use either Linux or Windows. AMI's toolset is designed to work seamlessly under both Windows and Linux.

Source File Views

VeB allows the engineer to view a project two different ways:

- File Explorer - A view of the files as they are stored in the project directory structure.

- Module Explorer - A view of the modules as they are logically organized by the module creators.

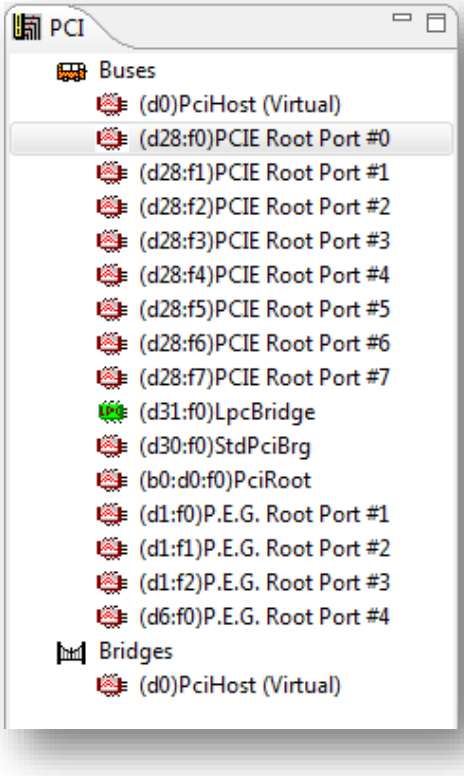
This very powerful feature allows the engineer to quickly navigate through the project to easily locate source code. The Module Explorer view also allows an understanding of how the project is organized, what modules/features are available in the project and allows for quick addition or removal of components.

Built in Editor

VeB includes a built-in editor which supports syntax highlighting and many other features available from the Eclipse source code editor. The user may configure VeB to use the built-in editor or to launch an external editor configured by the user. The VeB editor may be customized to use any hot key combination for common editing tasks which allows users to transition to the built-in editor.

PCI Objects Tab

VeB includes an advanced PCI configuration wizard. The PCI wizard describes the properties for PCI devices present on the platform. A summary of each object's parameters is displayed here. This screen also allows hardware engineers to set/verify interrupt routing, adding of option ROMs and associating ASL files with devices.



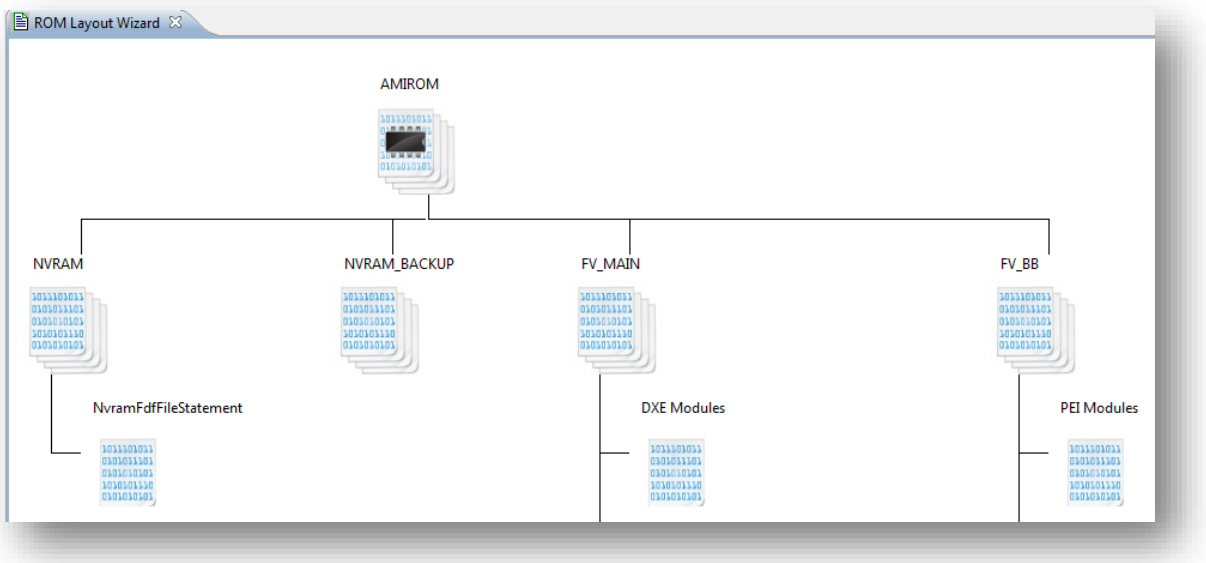
VeB also allows multiple views of the PCI layout. One view is through the PCI tab of the Tools panel, which shows the PCI space layout by bus or by bridge. This view is very useful for systems with complex PCI bus configurations.

With Aptio® V, AMI has expanded upon its features for PCI over previous versions. Common features include interrupt routing, ASL incorporation, wake capabilities, device type specification and option ROM incorporation. The new PCI features provide additional granularity for adding multiple ASL files for a single device, static resource assignment for a particular device or the entire system and customizable init routines for a device.

ROM Layout Wizard

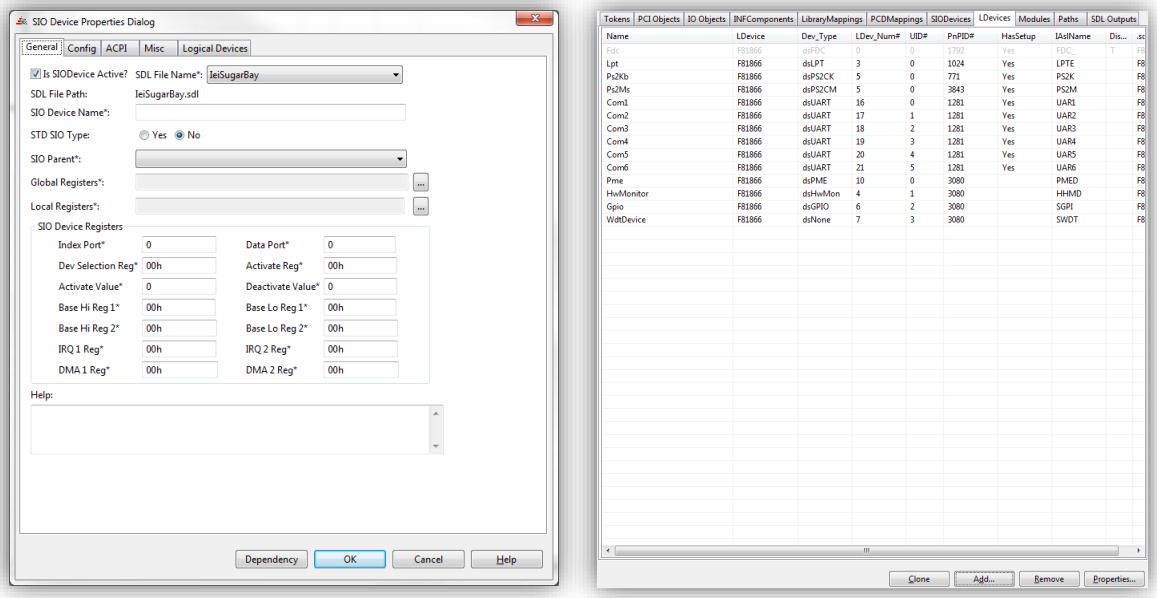
With the ROM Layout Wizard, engineers can create, edit and view ROM objects. The ROM layout wizard enables quick rearranging of the flash layout and size to meet custom requirements. The ROM Layout Wizard also allows easy reuse of a ROM layout from

project to project. This wizard's Graphical editor can be used on objects like FDINFO, FD_AREA and FFSFILE.



SIO Wizard

The SIO Wizard allows an easy ability to add support for any SuperIO. This wizard takes in the basic information of a SuperIO and does the rest of the work automatically. All that is needed is to give it the standard information of: Index/Data ports, Enter/Exit config mode, where registers are located, what are the global registers and ASL files for the SuperIO. A further wizard allows configuration of each LogicalDevice in a snap: the only code to be supplied is a custom init routine for LogicalDevices.



PCD Mapping

The PCDMapping tab displays the list of PCDMapping objects available in the current Aptio® V project. This allows the user to filter and view PCDs under selected architecture.

Platform Configuration Settings and System Description Language (SDL)

VeB includes a screen that allows the engineer to easily view and edit the settings of a device in BIOS parameters. BIOS parameters are analogous to the make flags used by previous AMIBIOS® releases. BIOS parameters data is stored within SDL files. SDL files are used to describe platform configuration settings that are used in the project build and/or by components source code. Each BIOS component includes at least one SDL file. SDL files define the parameters that are relevant to each individual BIOS component(s). Using VeB's BIOS parameter screen presents a graphical abstraction to platform configuration settings; this simple access makes it is unnecessary to directly modify underlying make files.

Project Build

A simple mouse click from within VeB builds the BIOS and displays any error messages that result from the build. The build output is displayed, by default, in VeB's lower pane. Double clicking on an error message in the window will causes the related file to be opened in VeB's editor.

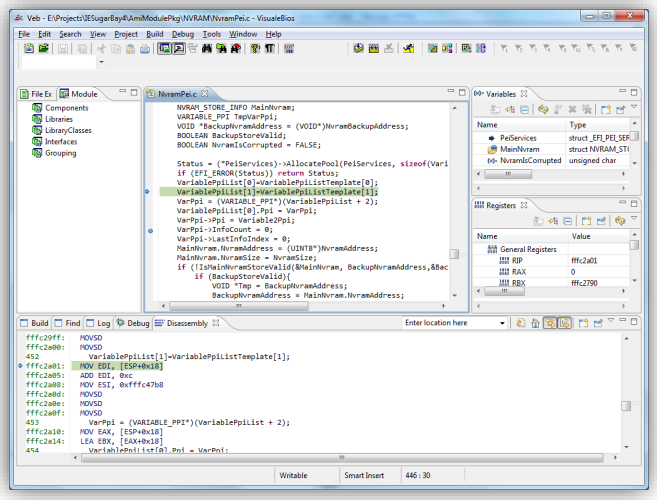
Context Sensitive Help

VeB includes a comprehensive help system for all chipset and OEM hooks. Pressing 'F1' while the cursor is located on the name of a hook function activates help for that function. Help includes a description of what the hook should do, who calls it, inputs and outputs,

etc. Over time, the help may also include useful hints or common pitfalls related to a particular chipset or OEM hooks.

AMI Debug for UEFI

AMI Debug for UEFI uses a flexible host/target configuration. The debug target communicates with a Microsoft Windows host application via RS-232 serial or USB 2.0 debug port. Originally developed as a debugger for EFI Shell applications, AMI Debug has been extended to support UEFI debugging in PEI, DXE, SMM and EFI Shell environments. AMI Debug for UEFI also integrates within VeB to provide a comprehensive development and debug solution.



- Source-level debugging
- Step into/Step over support
- Views: register, memory and variable
- Halt module support
- Breakpoint support

AMI Debug Rx

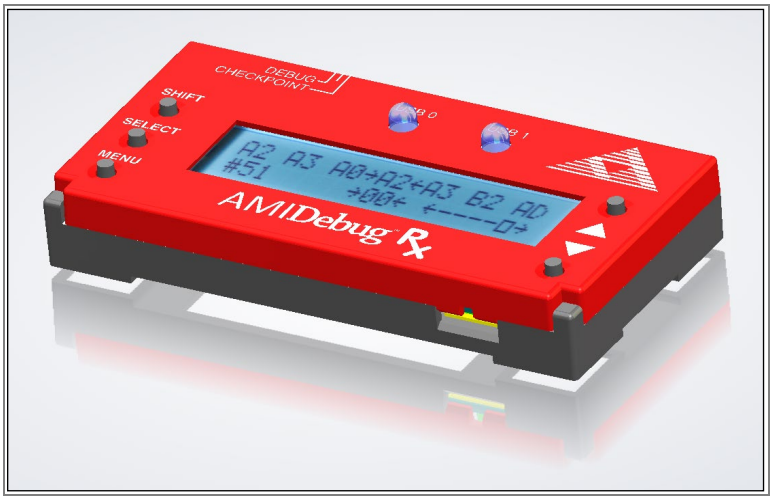
AMI Debug Rx™ is the first of its kind: a low-cost debug tool built around the debug port feature common to today's USB 2.0 EHCI controllers. Perfect for today's embedded, tablet and netbook platforms, this product is targeted to power users, quality assurance labs and service technicians. Diagnosing small form factor platforms with AMI Debug Rx is non-intrusive, allowing technicians to access checkpoints without opening the case.

AMI Debug Rx is designed as a replacement for the PCI "POST Checkpoint Card," which has become less useful in the PC market as newer systems omit the traditional PCI expansion slot.

Based on patent-pending technology, AMI Debug Rx replaces the POST checkpoint card's 7-segment LED with a small LCD screen. This debug method produces more descriptive debugging messages than the checkpoint card, includes boot performance timing and UEFI debug message redirection.

AMI Debug Rx Feature Set:

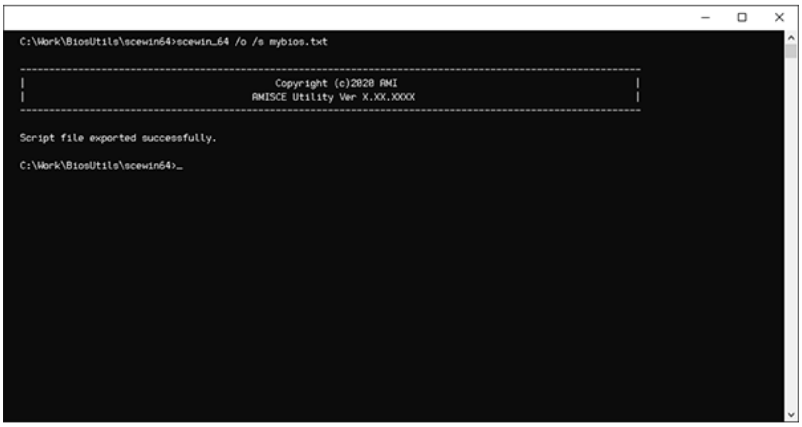
- Low-cost alternative to the PCI “POST Checkpoint Card”
- Low cost device for platform development or field diagnostics
- Device records checkpoints, UEFI debug messages and timing data for measuring boot performance
- Session data can be captured and stored to one of four “sessions” for later review
- Display descriptive text for each checkpoint: based on AMIBIOS8®, Aptio® 4.x or a user-provided string table
- AMI Debug Rx protocol can be ported into existing AMIBIOS8® and Aptio® 4.x BIOS projects
- Works with AMI Debug® for UEFI to enable source-level BIOS debugging
- Designed for BIOS developers, quality assurance testing and field diagnostics.
- AMI Debug Rx is available. For more information, contact an AMI Sales Associate.



Chapter 5 Aptio® V Deployment Utilities

AMI designs a variety of deployment utilities for Aptio, simplifying management of customer firmware images.

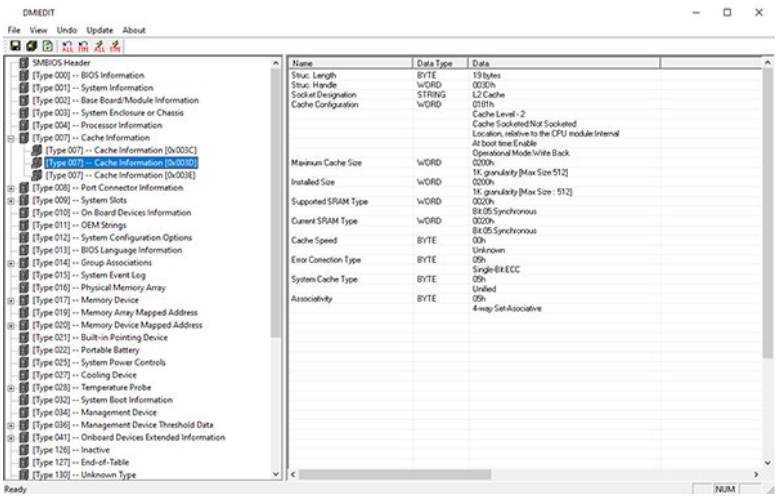
AMI Setup Control Environment (AMISCE)



AMISCE provides an easy way to update NVRAM variables, extract variables directly from the BIOS, change settings using either a text editor or a setup program and then update the BIOS.

- Supported in EFI Shell, Windows, Linux and FreeBSD
- Provides for the setup of the BIOS on targeted systems
- Scriptable for manufacturing environments

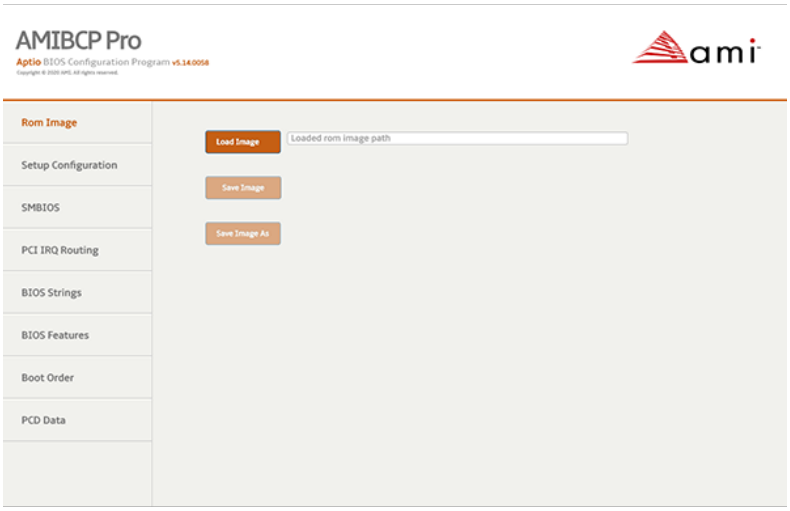
DMIEdit



DMIEdit is designed to modify platform-specific SMBIOS data in manufacturing environments. SMBIOS UUID, serial numbers, asset tags and OEM strings can be modified

using this script-driven utility. DMIEdit runs in Microsoft Windows and EFI Shell environments (32-bit and 64-bit).

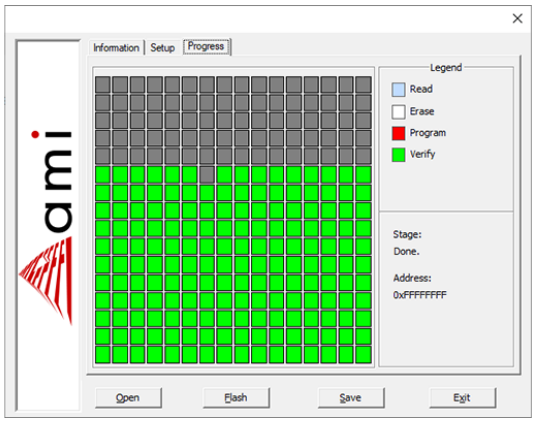
AMI BIOS Configuration Program (AMIBCP)



AMIBCP allows customers to modify common options in firmware ROM images without rebuilding the project from source code:

- Modify setup option defaults, multi-language strings and static SMBIOS Data
- Change setup option default values
- Change Unicode strings in setup and sign-on messages
- Edit static SMBIOS data

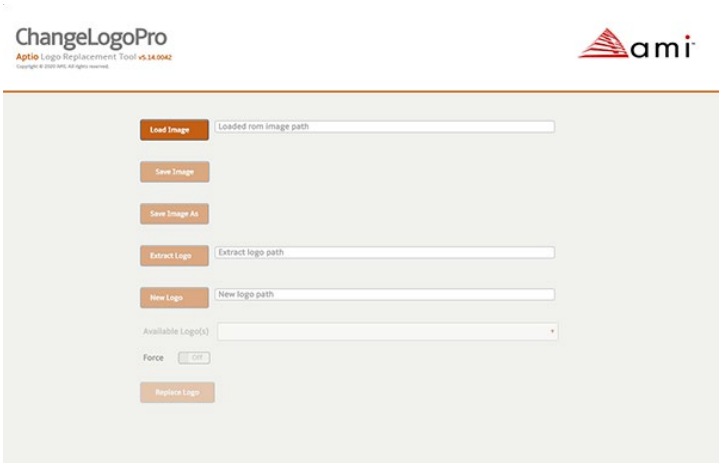
AMI Firmware Update (AFU)



AFU allows the system ROM to be upgraded from multiple operating environments.

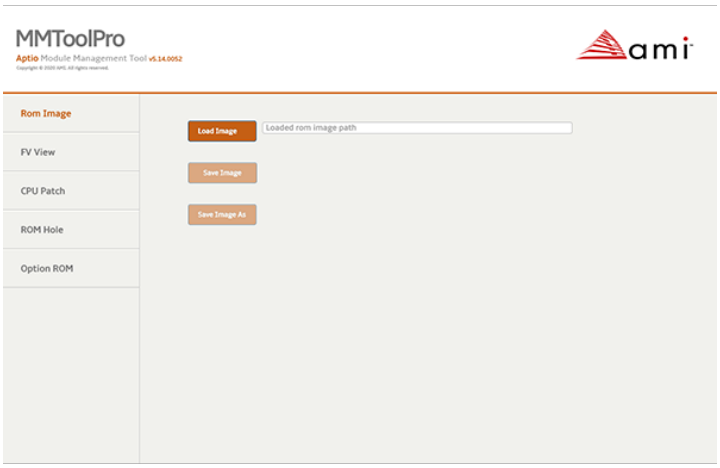
- Supported in EFI Shell, Windows, Linux and FreeBSD
- Command line utility – x86 and x64
- GUI version available for Microsoft Windows

ChangeLogo



ChangeLogo is Aptio's OEM logo customization utility. A platform's look and feel can quickly be changed by altering the "silent boot" logo embedded in the ROM image. ChangeLogo can also be used to extract logos from other Aptio® firmware images.

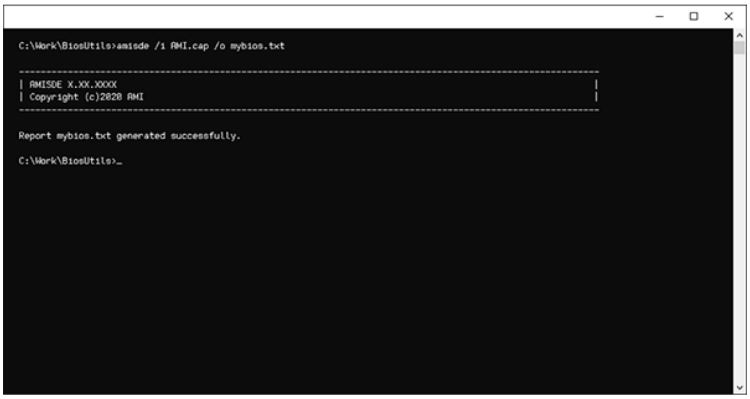
Module Management Tool (MMTool)



MMTool allows customers to manage the drivers and modules that construct an Aptio® firmware image.

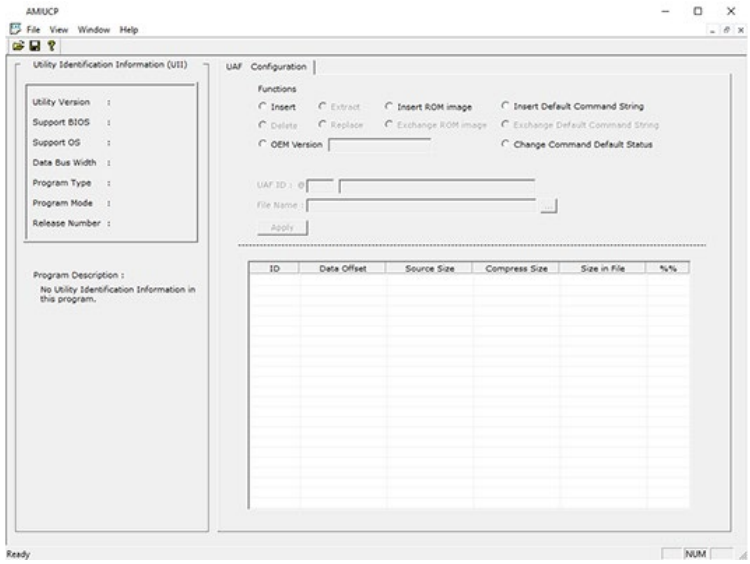
- Add, delete, replace and extract components without rebuilding from source
- Operates on PEI/DXE drivers and legacy Option ROM
- Command line interface available for automation in manufacturing environments

AMI Setup Data Extractor (AMISDE)



AMISDE is a command line tool for exporting setup data from an Aptio® ROM image. It produces a helpful summary report of BIOS parameters and default values that enhances productivity in testing and manufacturing.

AMI Utilities Configuration Program (AMIUCP)



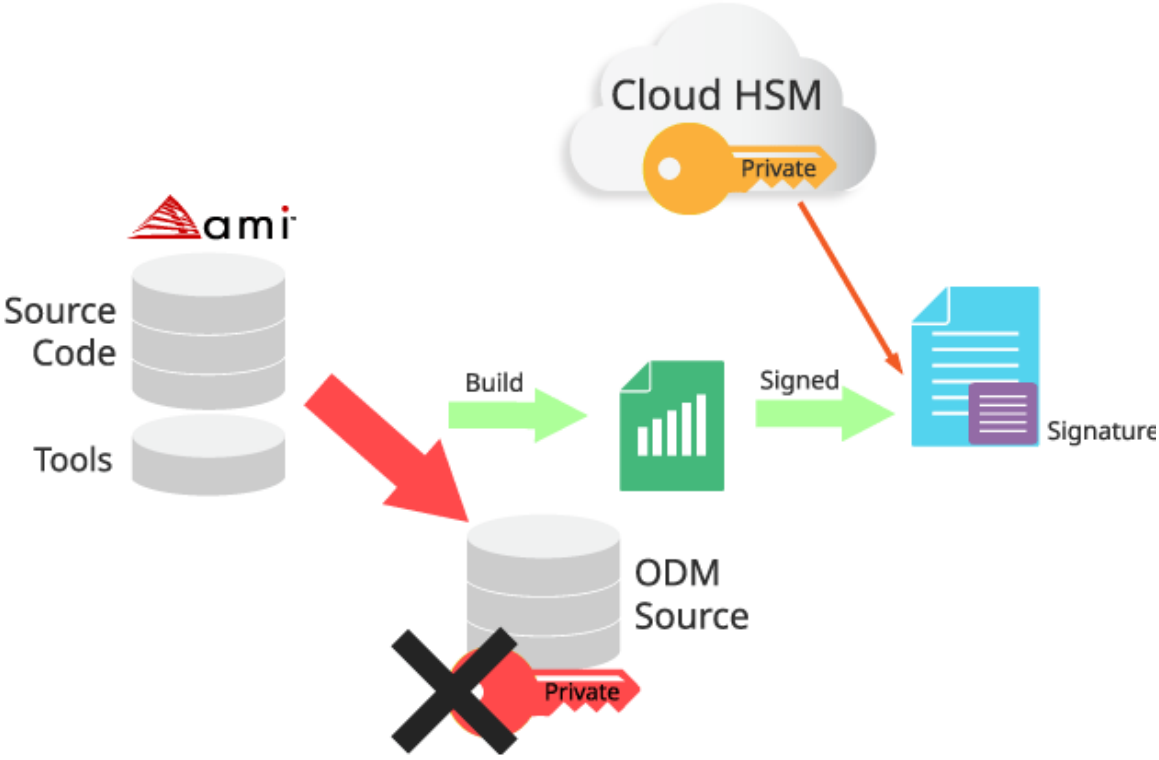
AMIUCP provides a means to pre-configure the AMI Firmware Update.

- Insert/exchange default command string for AFU
- Insert/exchange ROM image used with AFU
- Edit OEM version
- Change command default status

AMI Cloud Enabled Firmware Signing (CLEFS)

Having signing keys on each engineer's machine can be a security risk. These keys are most likely not protected in any manner and are more easily compromised. A Hardware Security Module (HSM) is the best solution for key management, but they are very

expensive, so AMI has partnered with Thales to offer a solution to enable signing for multiple industry standard technologies with cloud HSM integration. AMI CLEFS also allows for post-build signing and integration with on-site HSMs.



(Intentionally Blank)