



## Transitioning from Award BIOS & AwardCore

### Why transition from Award?

Due to the recent trends in the industry towards UEFI technology, Phoenix has renewed its focus on Tiano based products and is consolidating its support for legacy BIOS products along two superior product lines: Embedded BIOS® with StrongFrame® Technology and SecureCore.

Award Customers will greatly benefit from the transition to the following Phoenix products:

SecureCore Tiano: Phoenix has introduced a product called SecureCore Tiano that fully supports the Intel Platform Innovation Framework. SecureCore Tiano is designed to support industry leading chipsets and CPUs, and a wide range of third-party peripherals supporting UEFI/Framework drivers, fully leveraging the silicon vendors' chipset validation efforts.

Embedded BIOS®: Embedded BIOS® with StrongFrame® Technology is Phoenix's firmware SDK solution that has been specifically developed for embedded applications. It provides the fastest boot time in the market, a very small footprint and a mature and stable code base with over 1000 source level build options, making it the most flexible and configurable BIOS available.

Phoenix SecureCore™: SecureCore supports next generation silicon technologies such as hardware virtualization, iAMT (Advanced Management Technology), and TXT (Trusted Execution Technology). It is the BIOS code base with best support for current and next generation industry standards from a single code base. SecureCore includes additional security features such as support for multi-factor biometric authentication and StrongROM, an embedded cryptographic engine that can be used standalone or as a complement to TPM.

The rest of this paper describes the transition to UEFI and Embedded BIOS® with StrongFrame® Technology.

### Transitioning to UEFI

#### Bridging BIOS to UEFI

New versions of the computer's operating system (OS) get all of the attention, but there is also an evolution occurring in the core systems firmware that is responsible for getting things started on a PC. Often referred to as the BIOS (basic input/output system), this firmware is becoming a modular and configurable system element based on the Unified Extensible Firmware Interface (UEFI) standard that will give computer system developers a simplified method for incorporating new hardware technology and customizing system functionality. By following a thoughtful migration from the existing BIOS to this "BIOS of the future," developers will be able to gain this enhanced flexibility and functionality in future designs without compromising designs already in development.

In the earliest personal computers (PCs), the BIOS served primarily to provide the operating system with a standard view of the system's core hardware, including keyboard, mass storage, display, and serial I/O. The BIOS firmware told the central processor (CPU) how to read and control these resources and provided the operating system with a standard interface that hid variations in detail among various chipsets and peripheral devices. This gave PC developers freedom of choice in hardware options as well as an ability to add innovative features while assuring compatibility with the operating system's standard initialization process.

Over time the BIOS developed additional capabilities. Additions included power-on self-test (POST), power management, automatic enumeration and resource allocation for add-in peripherals, and a variety of system control and configuration functions. These additions came as a result of innovation by BIOS vendors and provided additional design flexibility and control options to system developers.

### **Opening the BIOS**

A desire began growing within the industry, however, to open BIOS innovation to others in the PC industry – especially silicon vendors. Opening the innovation process would provide greater opportunities for innovation within the PC industry by allowing more minds to work on the problem. It also would make it easier for system developers to differentiate their products by incorporating custom features in the BIOS. Silicon vendors also desired a faster method for incorporating new system hardware options into the BIOS. The traditional approach was for silicon vendors to hand over to BIOS vendors the firmware used to test new silicon, then wait for those drivers to be worked into the BIOS before offering the silicon to system developers. To speed this process, silicon vendors wanted a standard interface on which to base their drivers. This standard interface would allow the drivers to “plug in” to the BIOS without additional software design effort, eliminating the delays associated with integrating them into the BIOS and speeding the evolution of PC hardware.

The silicon vendor “wish list” for the BIOS continued to grow. There was a desire to be able to use a high level language such as C for driver development by standardizing on interfaces and coding practices, thereby easing driver development. The use of C would also help address a growing shortage of assembly language programmers. Another desire was to provide support of “pre-boot” environments that would give access to protected mode memory and allow address space management for software to run without requiring the operating system to be loaded. This feature would be especially useful in embedded computing applications that may not need full PC functionality and in automating the manufacturing test of PC hardware by enabling services for built-in self test.

One of the first attempts to create such expanded system firmware, now evolving far beyond BIOS, came from microprocessor vendor Intel. The company developed the “Platform Innovation Framework,” usually referred to simply as the Framework, as an architecture for system firmware development. Within that architecture Intel defined an Extensible Firmware Interface (EFI) as a standard for creating hardware drivers to work within the Framework. Working with Phoenix Technologies and other BIOS vendors, Intel incorporated EFI into the BIOS for its Itanium processor. The company further created a representative implementation it called Tiano to serve as a template for development and made the source code publicly available in order to promote the entire approach, which it referred to as “Green-H.”

Intel’s Green-H initiative met with objections from some quarters in the PC industry, however, because of several limitations. One was that the Framework and Intel’s EFI drivers were specific to Intel hardware architectures; the industry wanted a compatibility path for adoption of alternative hardware from other silicon vendors. The approach also did not address newly emerging technologies such as multi-processor configurations, and was slow to evolve, limiting opportunities for innovation.

Microsoft, as the primary OS vendor in the PC space, also wanted to have a say in how the firmware-to-OS interface looked like. Perhaps most importantly, the Intel specification could not be advanced without Intel’s approval and Intel revised the EFI specification only once, three years after its 1999 introduction. Intel currently has no plans to introduce any new versions of EFI.

### **UEFI arises**

In response to these limitations and restrictions, the PC industry formed in 2005 the Unified EFI Forum to develop broader firmware standards based on Intel’s EFI 1.10 specification, which it has licensed from Intel. In addition to broadening the hardware applicability of the concept behind Green-H, the Forum aimed to maintain the pace of innovation. UEFI 2.0 appeared in 2006 and UEFI 2.1 was introduced in January, 2007.

Firmware developed under the UEFI standard is a far cry from the traditional PC BIOS. Traditional BIOS is specific to the x86 architecture and needs to run under the 16-bit “real mode” of that architecture. It provides power-up hardware initialization and POST functions then serves as the interface between the hardware and the operating system. UEFI firmware serves some of the same functions, but is not a replacement for existing standards such as ACPI, SMBIOS, or the PCI firmware specifications. Instead, it enhances them by allowing simple incorporation of additional functionality.

UEFI-based firmware provides both boot services and run-time services. The boot services create a driver model for the devices used during boot, such as hard and floppy disk drives, network controllers, keyboards, mice and displays. The run-time services serve as the interface between the operating system and the hardware for low-level firmware functionality required during normal system operation. Rather than being hard coded and hand packed like the BIOS, however, UEFI-based firmware follows a modular approach that allows system developers several approaches for augmenting its functionality.

At the hardware level, the UEFI specification gives chip developers a standard interface so that they can create a firmware driver plug-in to handle their specific boot hardware. System developers can then take UEFI-based firmware and add the drivers for the hardware they selected without needing to do any additional program development. At the software level, the specification gives system developers a method for augmenting the firmware with their own code. Because the UEFI specification ensures that a simple, linear, protected memory addressing mode becomes available early in the boot process, developers have access to a well-defined pre-OS environment that they can use to run custom code for such things as manufacturing tests, system diagnostics, or provisioning functions.

Developers can also use the pre-OS environment to configure the system for embedded operation without requiring that it include normally essential PC features such as a keyboard, mouse, or monitor.

### **UEFI advantages**

As a result of the ease with which the UEFI-based firmware can be adapted, adopting the standard gives developers a number of advantages. One is to simplify the incorporation of new hardware technology as it becomes available. The only software impact of adding new hardware is adding a new driver to the firmware. Customization also becomes simpler. Vendors can create UEFI drivers to provide features and functions unique to their system and simply add them to the firmware.

This ease of customization is especially beneficial for systems that are developed to serve a low-volume market, such as a handheld computer for a shipping company that includes proprietary functionality and does not run a traditional OS. Creating such a system, while using a traditional BIOS, would require considerable software development. Under a UEFI system the development costs are considerably lower.

The adaptability of UEFI-based firmware also gives system developers more freedom of choice. They can create their customizations once then apply them to the UEFI firmware of whatever board design they choose. This simplifies switching between in-dependent board vendors by virtually eliminating the firmware impact.

While the advantages of UEFI-based firmware are compelling, developers face a significant challenge to adopting the approach: time. Product development time for PCs average nearly 18 months, and server-class system often take longer. As a result, the development of many systems began well before the UEFI Forum released its specification to replace EFI. The development time for new silicon is also long, so the devices currently on the market were created before the UEFI specification became available. As a result, very few UEFI drivers exist for today’s silicon. Similarly, mainstream OS also lack support for UEFI firmware.

### **Building bridges**

As a result, the systems currently in development as well as those now starting will still require traditional BIOS support. Further, the need for a traditional BIOS will continue for a number of years while the industry is

transitioning between the standards. Until all the necessary chips have UEFI driver support, operating systems are able to tap into UEFI run-time resources, and the market has discontinued the use of older, unsupported devices, developers will be caught in a “mix-and-match” situation where their systems will have a blend of supported and non-supported components. To meet their needs during the transition time, system developers will need firmware that bridges between the traditional BIOS and UEFI-based operation.

Phoenix Technology offers such a bridging solution: the SecureCore BIOS. This firmware is in full compliance with the UEFI 2.0 standard and is compatible with Intel’s Tiano/Green H implementation and proprietary EFI drivers. It works with Intel’s and AMD’s upcoming chipset platforms, Windows Vista, XP, and earlier operating systems, and classic silicon drivers. SecureCore guarantees support for today’s silicon, eliminating the “mix-and-match” challenge. It also guarantees support for current OSES as well as forthcoming UEFI-aware OSES. Phoenix has already demonstrated SecureCore’s compatibility with Microsoft’s efforts at a recent Plugfest.

The industry’s move to UEFI is now becoming inevitable. Intel is targeting incorporation of UEFI compatible drivers into its reference platforms for the next-generation hardware chipsets and has discontinued major development on its proprietary EFI standards. AMD is also embracing UEFI 2.x, offering for its new CPU and chipsets UEFI drivers that Phoenix already supports. Microsoft has made Vista UEFI-aware and will support the standard in its forthcoming Longhorn server software. Major independent hardware vendors for plug-in I/O hardware have also adopted UEFI for driver development. The UEFI standard is thus being taken up by the major PC vendors, and others will have to follow in order to remain competitive. With offerings like SecureCore, Phoenix Technology is helping developers prepare for full adoption of the UEFI standard in future generations of PCs.

As a world leader in BIOS software development, Phoenix has in-depth understanding of the features and functions that will need to remain available during the transition. At the same time, its leadership position within the UEFI committees ensures that it has advanced understanding of where the industry is headed. With this combined background it has been able to develop SecureCore to be just what the industry needs just when it needs it.

### **Transitioning to SecureCore Tiano**

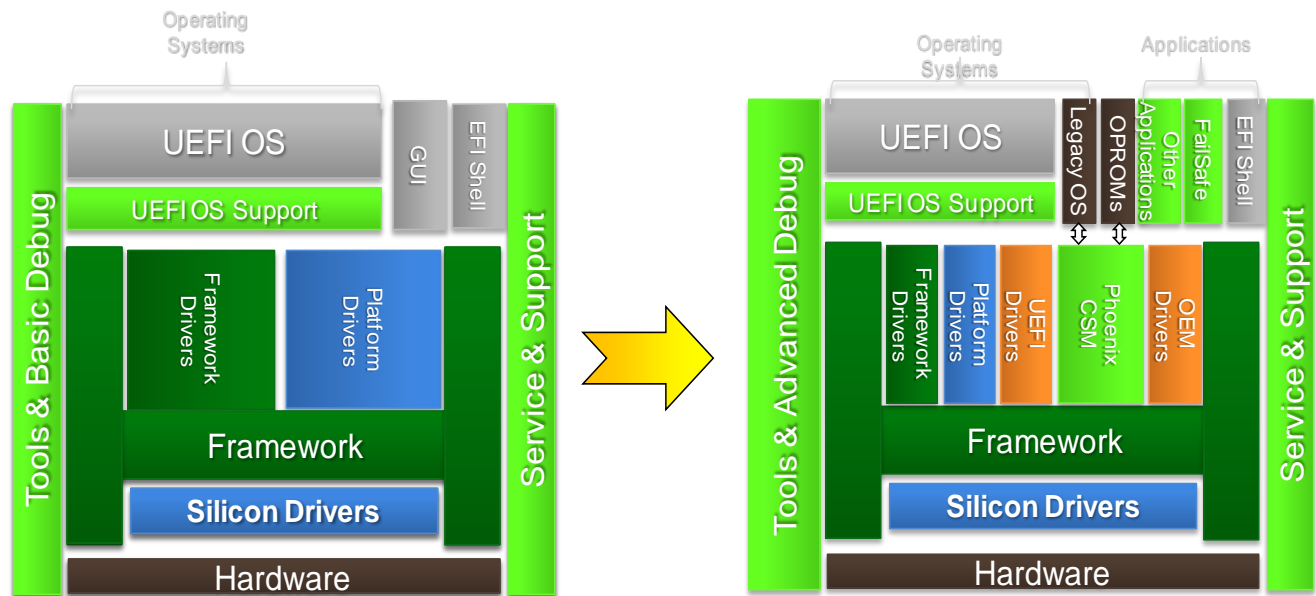
Phoenix has utilized the benefits of the new modular and more easily extensible codebase to rapidly implement support for a faster, more secure BIOS called SecureCore Tiano.

SecureCore Tiano fully supports the Intel Platform Innovation Framework and is Phoenix’ flagship, bit-for-bit EFI compatible BIOS family of products. SecureCore Tiano is designed to support industry leading chipsets and CPUs, and a wide range of third-party peripherals supporting UEFI/Framework drivers, the latest industry hardware standards, virtualization, a rich set of pre-OS applications, and tools that decrease BIOS enablement time and cost for new customer platforms by speeding up the debugging and validation processes.

To help ease the shift that system developers must make between the traditional BIOS and UEFI based firmware, SecureCore supports their existing assembly language code-base and will accept many of their current firmware customizations. Developers can work with SecureCore using mixed mode tools such as Visual Studio 2005 that understand both assembly and C code, allowing them to merge their existing firmware with SecureCore’s code without re-coding. This gives developers time to move from a traditional to a UEFI-based approach gradually, in phases.

Customizations that were done on older legacy BIOS products can be easily supported on SecureCore Tiano by the Compatibility Support Module (CSM). Customizations that were implemented using legacy OpROMs will be supported by the CSM. The CSM also allows the booting of a traditional (i.e.) non-EFI-aware operating systems. It also allows the loading an EFI-aware OS a device that is controlled by a traditional OpROM.

Customizations can also be done by OEM's developing their own UEFI drivers to provide features and functions unique to their system and simply add them to the firmware.



### **Transitioning to Embedded BIOS**

Phoenix Technologies' Embedded BIOS brand pre-boot firmware is the premium firmware used by most makers of embedded x86 equipment today to support embedded hardware. Embedded BIOS® with StrongFrame® Technology is Phoenix Technologies' sixth generation BIOS Technology, selected for its superior combination of configurability, functionality and extreme Ease of Use.

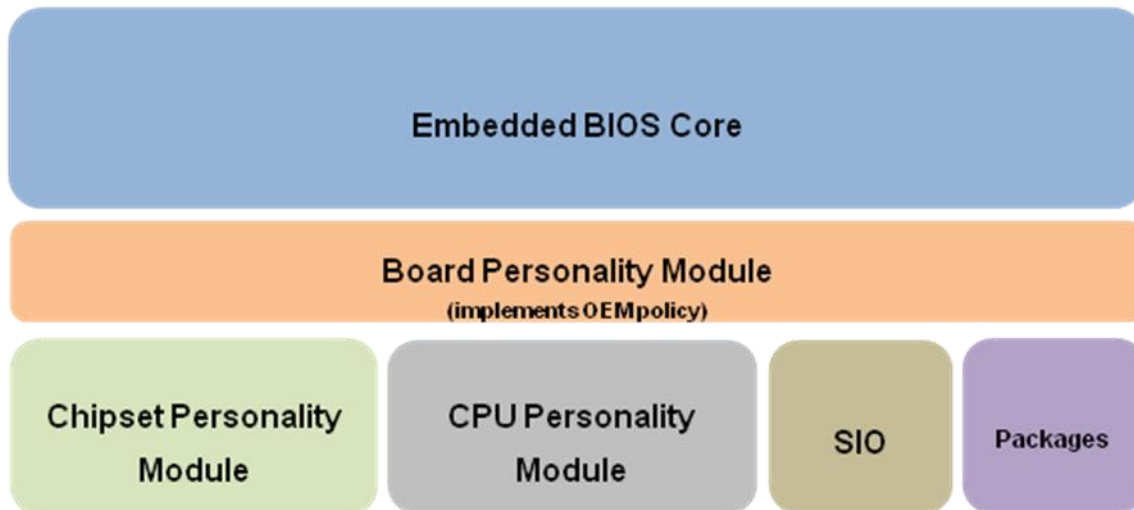
The BIOS in a typical PC provides the same standard user experience for the systems it runs on. This allows a wide range of users to intuitively use any notebook computer, regardless of brand, for example. Embedded BIOS can be configured to emulate the PC desktop or server experience; however, this is only one approach to interacting with the user, and it may not be the most appropriate one for a more specialized product. With over 1,000 ways of being configured by the OEM, it enables differentiation of products from competing products in quick and cost effective way.

The Embedded BIOS SDK comes with full source code for the entire BIOS core. One benefit to the ODM/OEM customer is full transparency in the core, allowing the customer to gain greater knowledge of the internal operation of the core through well-documented source code. Another benefit is that a full-source core allows the code to be rebuilt during the BIOS build process, and this means that configuration options can selectively include or exclude code paths to build a highly-tailored binary image.

The SDK also includes some binary components that aren't a part of the BIOS itself, such as the Firmbase® Technology kernel and its USB stack, High Availability Stack, and other Firmbase Technology components. These binary components by their nature are cross-platform compatible and offer the lowest risk to ODM/OEM customers when supplied as binaries already pre-tested across a broad spectrum of silicon and OS architectures. Source code to these components is available directly from Phoenix Technologies under separate licensing arrangements.

The Embedded BIOS core architecture provides the flexibility of supporting OEM-level customizations very easily. The functional diagram of Embedded BIOS is below

## Embedded BIOS Functional Diagram



The policy decisions are implemented in the Board Personality Module (BPM). All of the policy decisions that are typically implemented by the core are called out into a single entity called the BPM. This means that the OEM/ODM can implement the custom policy in a single file. The BPM callouts, which commonly execute default routines inside the core, may be intercepted by the OEM's BPM, and custom coding may be created to handle customization.

This architecture minimizes the BIOS expertise level required by the programmers to create customizations to suit their applications making the transfer of customizations done on Aware codebase to Embedded BIOS very simple and straightforward.

### **How can Phoenix assist you in the transition?**

Phoenix is committed to ensuring a smooth transition for our Award customers to our newer products and can provide substantial support and training to development teams during this transition. We have detailed technical training classes to train BIOS developers on to SecureCore Tiano or Embedded BIOS.

For customers migrating to UEFI technology (SecureCore Tiano), Phoenix can ensure customer's success by engaging with the customer very early during the design cycle, significantly shortening the development time by working with Intel and the customer to facilitate communication and resolving issues faster. This multi-pronged approach will result in faster TTM and better product quality for the customer.

Please contact your local Phoenix account representative for additional details.