



**Secure** from the **START**

# Phoenix TrustedCore™ SP3b

## Supports TPM 1.2, Microsoft Vista BitLocker, Preboot Authentication, Microsoft FlexGo and UEFI 2.0

Phoenix TrustedCore SP3b proactively protects x86-based computing devices and their data before the operating system and applications even load, creating a secure, tamper-resistant platform.

For desktop, mobile, embedded and server systems, and consumer devices, TrustedCore SP3b incorporates sophisticated firmware security enhancements that fundamentally transform legacy BIOS technology.

### Industry Leadership at the Core of the Device

With Phoenix TrustedCore™ SP3b, Phoenix continues its industry leadership in providing a platform for ensuring that PCs, notebooks, embedded systems, servers and embedded servers meet current and emerging security standards and requirements.

Phoenix TrustedCore SP3b supports the Trusted Platform Module (TPM) 1.2 specification and is the first firmware to fully implement key industry standards required for Microsoft® Windows® Vista™. TrustedCore SP3b support of the TPM 1.2 specification helps ensure that malicious code cannot invade a device early in its boot process.

TrustedCore SP3b includes support for the Unified Extensible Firmware Interface (UEFI) 2.0 specification. The UEFI specification is part of an industry initiative to ensure a transparent interface between a device's operating system and the platform firmware at boot time. In addition to UEFI boot loader, TrustedCore SP3b also fully supports UEFI silicon drivers for either PIWVG or Intel Tiano (Green H).

Phoenix has also created a preboot authentication standard, based on a set of application programming interfaces, that allows for easy integration of third-party two-factor authentication devices, such as biometric fingerprint sensors and smart tokens. This standard ensures that endpoint devices are not only virtually tamper-proof, but also easy to build.

In addition, Phoenix TrustedCore SP3b includes an enhanced embedded cryptographic engine, called StrongROM, which allows authentication of firmware. StrongROM can complement TPM 1.2 chip technology to further enhance device security or provide a level of cryptographic security by itself for systems that do not contain TPM 1.2 compliant chips.

Phoenix leads the industry in providing master boot-record authentication at the firmware level, which prevents tampering with the operating system or the hard disk. Targeted for specialized applications and embedded systems, master boot-record authentication provides a trusted boot path for the entire operating system, and can enhance the endpoint security and core root of trust for Microsoft Vista™ BitLocker™ as well as Microsoft FlexGo™.



## TrustedCore SP3b enhancements

- TPM 1.2 for Windows Vista BitLocker logo compliance – Phoenix TrustedCore SP3b is the first firmware offering full compliance for the Trusted Platform Module 1.2 specification. TPM 1.2 is an essential level of compliance for secure start of Microsoft Windows Vista, scheduled for release in late 2006. Phoenix support of the TPM 1.2 specification helps ensure that malicious code cannot invade a device early in its boot process.
- StrongROM authentication of CSS – Phoenix TrustedCore SP3b includes the embedded cryptographic engine, StrongROM, which allows authentication of the firmware itself. Starting at the firmware level, TrustedCore SP3b provides a secure root of trust for operating systems such as Windows Vista. StrongROM can complement a TPM 1.2 chip in a system to further enhance device security, or provide a level of cryptographic security by itself for systems that do not contain the TPM 1.2 chip.
- UEFI 2.0 – Phoenix fully supports the Unified Extensible Firmware Interface 2.0 industry standard. For more information on UEFI go to [www.uefi.org](http://www.uefi.org).
- Microsoft FlexGo – Phoenix supports the Microsoft FlexGo technology & business models for computing devices through the optional TrustedCore module, Phoenix TCSUBscribe™. TrustedCore SP3b, together with TCSUBscribe, form a software-based secure execution environment to support secure metering functions for Microsoft FlexGo, and works with industry standard x86 CPUs and chip sets.
- TrustedCore Preboot Authentication – Phoenix has created a preboot authentication standard, based on a set of application programming interfaces, that allows for easy integration of third-party two-factor authentication devices, such as biometric fingerprint sensors and smart tokens. The optional TrustedCore Preboot Authentication module works with TrustedCore SP3b.

## TrustedCore SP3b provides a wealth of desirable security features

TrustedCore SP3b includes numerous enhancements that increase the functionality of the TrustedCore product line. A member of Phoenix award-winning product lines, TrustedCore SP3b is designed for OEMs and ODMs and embedded systems' vendors developing hardware products using x86 silicon technologies. It leverages Phoenix CoreArchitect™ to provide rapid deployment of systems with extensible system security and management features.

## TrustedCore SP3b benefits for OEMs, ODMs, and system builders:

- Build feature-rich devices that stand out from the competition
- Speed time to market with targeted core-enabled applications
- Reduce development costs with proven system software
- Reduce support costs by building self-healing functionality into devices
- Streamline integration with robust development and debugging tools such as Phoenix CoreArchitect 2
- Leverage development resources with a single product family that supports PCs, notebooks, servers and consumer devices

For the latest technical specifications visit us at [www.phoenix.com/trustedcore](http://www.phoenix.com/trustedcore)

### Phoenix Technologies Ltd.

915 Murphy Ranch Road  
Milpitas, CA 95035 USA  
408.570.1000 main  
408.570.1001 fax

800.446.9202 North America sales  
781-BUY PTEC Outside North America sales

©2006 Phoenix Technologies Ltd. Phoenix and Phoenix Technologies are registered trademarks of Phoenix Technologies Ltd. All rights reserved worldwide. All other brand or product names are the trademarks and property of their respective holders.