Phoenix SecureCore Technology™
Server Solutions

Phoenix SecureCore Technology™ (Phoenix SCT) is the next-generation UEFI BIOS firmware of choice for servers, offering power-efficient performance, remote manageability and advanced security. Designed with over 30 years of domain expertise in firmware architecture and engineering, Phoenix SCT is the first UEFI BIOS with native EDK II support that is also compatible with EDK 1117.

Intelligent Computing for Servers and Cloud Platforms

Designers of data centers and server clusters must now be concerned with more than just availability, scalability and reliability. Ever-increasing demand for greater power efficiency, remote manageability, and advanced security is a major concern for telecom operators, communication or Internet service providers, and enterprise IT departments alike. Data is a strategic asset for many organizations and network resources need to be protected against unauthorized access and malicious attacks with vulnerability-resistant platforms and innovative security technologies.

Phoenix SCT is an intelligent firmware solution designed to cover all these security threats. Phoenix SCT provides advanced networking and security features with a proven firmware architecture designed for scalability and portability. Optimized for mission-critical server applications, Phoenix SCT is the most dynamic and reliable UEFI firmware solution on the market.

Security

Equipped with Phoenix Pre-Boot Authentication (PBA) and compliant with industry-leading specifications like TCG 1.2, TPM 2.0, NIST-SP800-147 and Secure Boot, Phoenix SCT offers a strong security kernel to protect the core system software from malicious attacks and unauthorized firmware updates.

Manageability

Phoenix SCT enhances remote manageability by supporting comprehensive server manageability standards and technologies like Intel Node Manager, BMC support through Intelligent Platform Management BUS (IPMB), Intelligent Platform Management Interface (IPMI), Data Center Manageability Interface (DCMI), Serial Over LAN and Intel vPro technology.

Reliability, Availability and Serviceability (RAS)

Extending mean time between failures (MTBF) and eliminating unplanned downtime is mission critical for server operation. Phoenix SCT ensures data integrity and optimizes event handling with RAS features like ECC, scrubbing, sparing, scrambling, mirroring, poisoning, and lockstep mode.

Applications

Communications
Cloud Computing
Enterprise
Small to Medium Business

Foundation

Native EDK II Support with EDK 1117 Backward Compatibility

- Supports Built Systems based on EDK 1117 Patch V7, V8, and UDK 2010 SR1

Full Compliance with the Latest Industry Standards

- UEFI 2.3.1, PI 1.2, TPM 2.0, ACPI 5.0, TCG 1.2, NIST-SP800-147 and SMBIOS 2.7

Feature Highlights

Clean Code Tree Layered by Modularized Structure

- Modular Source Tree Structure - SDK
- Quick Reference Code Drop-In
- Extensive Silicon Support Library

Feature-rich and Touch Optimized Design

- Connected Standby Ready
- GUI Setup and Touch Hot Zone
- SMI free Runtime Service Support
- Safe Recovery BIOS[2]
- VFR Style Boot Page
- Non-volatile Capsule

Industry Leading UEFI Security Features

- Secure Boot: Signature Auto-Enroll
- Secure Boot: Windows 8 Key Management
- Secure BIOS: Lockdown SPI
- Security Variable Protection

Development Tools

- Phoenix CoreArchitect™
- Tool Development Kit
- Tools Subscription Program
- Phoenix Debug Device Reference Design


Universal Build System


Windows 8 Readiness


GUI BIOS Setup


Greater Security


Touch Enhancement


Boot Experience

Server Features

- Memory ECC and Patrol Scrubbing
- Memory Mirroring and Failed DIMM Isolation
- Intel Data Direct I/O(DDIO)
- AES-NI
- Intel Node Manager
- Intel Data Center Manageability Interface (DCMI)
- APIC Virtualization (APICv)
- MCA Support and Event Log

General Features

- Built-in UEFI Shell and UEFI Protocols
- SMBIOS 2.6/2.7 Support
- Event Logging
- Multi-Version SMBIOS
- SLP 2.0/2.1 and OA3.0 Support
- Compatibility Support Module (CSM) Support
- Up-to-date I/O Support
- Legacy I/O Support: Floppy, LPT, Serial Port, PS/2
- Multi-Language Support
- Console Redirection
- Debug Driver for PEI/DXE/SMM
- Crisis Recovery
- Touchscreen Support

Boot Manager

- UEFI/Legacy Boot Option
- VFR Style Boot
- Boot Device Auto-Detection and Adding to Boot Order
- Multiple Boot Device Support: HDD, CD-ROM, USB, LAN, SATA, ATA RAID, SD, eMMC

Security

- TPM 2.0
- TCG 1.2
- Microsoft Windows 8 Secure Boot
- Microsoft BitLocker
- Microsoft Windows 8 eDrive
- Multilevel BIOS Password
- Intel Identity Protection Technology (IPT), Intel Anti-Theft Technology (ATP), Trusted Execution Technology (TXT), Execute Disable (XD), AES

Virtualization

- Intel VT-d, VT-x, PCIe SR-IOV

Platform Management

- IPMI 2.0, DASH, Serial Over LAN, ASF, ECC Error Handler, BIOS Capsule Update, Intel AMT/vPro

USB Support

- USB 1.1/2.0/3.0
- UHCI/OHCI/EHCI/XHCI Mode
- USB Device Hot Plugging
- IRQ-Based Legacy USB Devices
- SMI-Based Legacy USB Devices

ACPI Support

- ACPI 3.0/4.0/5.0 Compliant
- Power States: S1/S3/S4/S5
- HPET
- Simple Boot Flag (SBF)

BIOS Setup Support

- Text Mode Setup
- GUI Setup
- OEM Logo/Setting Customization

Why ELTAN

Professional Design support for your system solutions
Experienced European Development team

- Superior UEFI BIOS engineering
- Direct engineering contacts for fast support and ensure you go to market
- Hundreds of embedded systems projects completed
- Hardware and Embedded Controller Design
- Device Driver and Operating System Experts
- Quality, Reliability, Extended lifetime support
- Co-operating with Intel, AMD and other Silicon Vendors

Phoenix Technologies Authorized Distributor

ELTAN B.V.
Ambachtstraat 23, 5481 SM Schijndel
The Netherlands
Tel +31 (0)73-5944660
Fax +31 (0)73-5941187
E-mail Info@eltan.com
Website www.Eltan.com