

Overview

Phoenix TrustedCore™ Embedded

A Secure Platform for Embedded Systems Development

Phoenix TrustedCore Embedded – The Chain of Trust

Phoenix TrustedCore Embedded is a next-generation, secure platform for embedded systems development and deployment. It is a unique and sophisticated solution that removes the risks of networked embedded systems by surrounding the device, the user, the application, the operating system, and the network with built-in and seamless protection to stop intruders from compromising the system.

The power in this solution is its integrated, layered security, creating a chain of trust, which is essential to any networked device. The chain of trust relies on certified and authenticated relationships between devices, networks, users, data, and applications. The following table shows the Phoenix protection layers and related trust modules that can be applied to create an ironclad chain of trust.

locks the flash part on the motherboard to prevent unauthorized updates. When a flash upgrade operation is performed, SecureFlash accesses the new core system software's digital signature to authenticate that the core system software image is correct for the motherboard—authorized and intact. Upon successful authentication, the flash part is reprogrammed and the new image is locked down as before. Access to the Phoenix core system software is denied if the credentials do not authenticate. SecureFlash acts like antivirus software for the Phoenix core system software, but with an important difference. Instead of detecting and quarantining viruses after infection, SecureFlash stops worms and viruses from ever reaching the core system software.

Protection layers	PHOENIX TRUST MODULES*			
	StrongRom	SecureFlash	TrustConnector	cME
Device configuration	•	•		•
Data and credentials to application	•	•		
Data and credentials to device	•	•	•	•
Application integrity	•	•		•
Device to network	•	•	•	
Application to network	•	•		

* Includes a full suite of development tools

TrustedCore Embedded and StrongROM module—the first link in the chain of trust

Phoenix TrustedCore Embedded is the foundation for the chain of trust which enables security, manageability, connectivity, and usability for networked embedded devices. It contains the Phoenix StrongROM™ trust module which is the lynchpin that binds device and application authentication services to storage available in the silicon of the device. With TrustedCore Embedded, the device and the data are proactively protected before the operating system and applications even load.

The Phoenix StrongROM trust module is a firmware-based crypto engine that protects application, user, and device authentication credentials using tamperproof core system software (see Phoenix SecureFlash—the second link in the chain of trust), rather than on easily attacked hard drives. No additional security processors are needed—no tokens, no smart cards. Because it is built-in, it is always on to seamlessly protect embedded systems against denial of service attacks, accidents, and mischief. Based on the needs of your customer and the device, you have complete control to transparently enable or disable StrongROM protection as needed.

Phoenix SecureFlash—the second link in the chain of trust

Phoenix SecureFlash is a utility for TrustedCore Embedded that protects the core system software from being reflashed with incorrect or malicious code. It works in conjunction with the StrongROM cryptography function to authenticate digital signatures. Each time the system is booted, SecureFlash

Phoenix TrustConnector—the third link in the chain of trust

Phoenix TrustConnector is a universal cryptographic service provider (CSP) component for Microsoft Windows embedded systems. It uses the StrongROM module to protect credentials that can be used to identify and authenticate the device as it connects to the network or for any other purpose. The authentication can happen at multiple network levels—at the switch, at the antivirus server, at the directory server, at the VPN gateway, and more. TrustConnector gives you the assurance that the credentials cannot be stolen or copied to another device.

TrustConnector interfaces with the Microsoft CryptoAPI and with StrongROM. Because of this integration, Windows, Windows applications, devices, users, and the network are seamlessly tied together for enhanced protection of identity credentials below the operating system.

Phoenix Console 2004 — the fourth link in the chain of trust

The Phoenix cME Console Platform 2004 is a flexible, tamper-resistant environment for delivering must-have applications and system services. It is the countermeasure to offset the impact of malicious attacks and corrupted applications, ensuring that data and applications are kept safe from catastrophes.

The Phoenix cME Console Platform is operating system independent (OS) and can't be overwritten by the operating system or by malicious activity. It includes a graphical user interface, a protected pre-OS workspace, and certified applications and Platform services.

Phoenix TrustedCore™ Embedded

The cME user interface controls the launch of the cME Console services and certified applications, even when the operating system will not boot. It is graphical in nature and can be easily customized to meet the design and branding requirements of each customer and device.

The protected pre-OS workspace is a secure area on the hard drive for services, data, and certified applications. The workspace is either a host protected area (HPA) that is totally invisible to the operating system and defended by the firmware and the hard drive, or a hidden, but OS accessible Phoenix Protected Partition, which in Windows environments is secured by the Phoenix Guardian firewall.

Certified applications and Platform services complete the environment, delivering system diagnostics, disaster protection, and other functionality that can be customized for each customer and device. By using Phoenix cME applications and Console services, critical devices and data can be easily recovered if they should malfunction or be attacked by malicious activity. The Phoenix cME Console 2004 includes a comprehensive deployment suite that makes cME Console 2004 development, integration, modification, and enhancement easier for faster time to market and added security. Phoenix cME Console services and applications include:

- Vault- —an application reinstallation service that does not need software CDs
- Phoenix FirstWare Recover Pro 2004 — a certified application for system and data restoration that does not need a boot disk or recovery CD
- cME Integration Kit—a development tool for the creation of third-party certified applications (see TrustedCore Embedded development tools)
- Phoenix System Deployment Kit—enables installation of the Phoenix Console Platform

Phoenix TrustedCore Embedded development tools

To make the chain of trust easier to develop and deploy, Phoenix offers a range of development tools. With these tools you can create and customize next-generation embedded systems to meet the needs of your customers.

CoreArchitect™—an advanced, integrated development environment (IDE) for TrustedCore Embedded core system software. Based on the industry-standard Microsoft Visual Studio .NET Professional application, the CoreArchitect plug-in adds a complete, fully integrated tool suite and a customized GUI specifically for Phoenix core system software development. With CoreArchitect, embedded system designers can simplify and accelerate product design and testing; easily integrate Phoenix StrongROM, SecureFlash, TrustConnector, and security features; and build devices that offer greater trust, manageability, connectivity, and usability.

Phoenix Security SDK—integrates StrongROM device authentication and security functions into custom applications

Phoenix Trusted Partner Network – A Partner Ecosystem for Faster Development

The Phoenix Trusted Partner Network is a worldwide group of Phoenix-trained network of engineering, motherboard, and device OEM partners. These partners are leaders in solutions for the embedded market and maintain firmware engineering, software customization, and deployment as core competencies. Phoenix works closely with these worldwide partners to keep them abreast of the latest firmware advances, industry standards, and feature-set technologies.

Features at a Glance

Key Features

- A complete solution that includes firmware, development tools, and managed applications
- Multilayered device, user, and application authentication, delivering a chain of trust from the core system software to the network
- A wide range of boot options, including multiple media types, network boot, Multiboot XP, and Remote Multiboot XP
- Device interface customization, including multimedia, JPEG, and BMP images
- Phoenix StrongROM tamperproof firmware-based crypto engine
- Phoenix SecureFlash protection for the core system software
- Phoenix TrustConnector protection for the device and the network
- Phoenix cME Console 2004 trusted application environment
- Phoenix FirstWare family of system management and recovery software

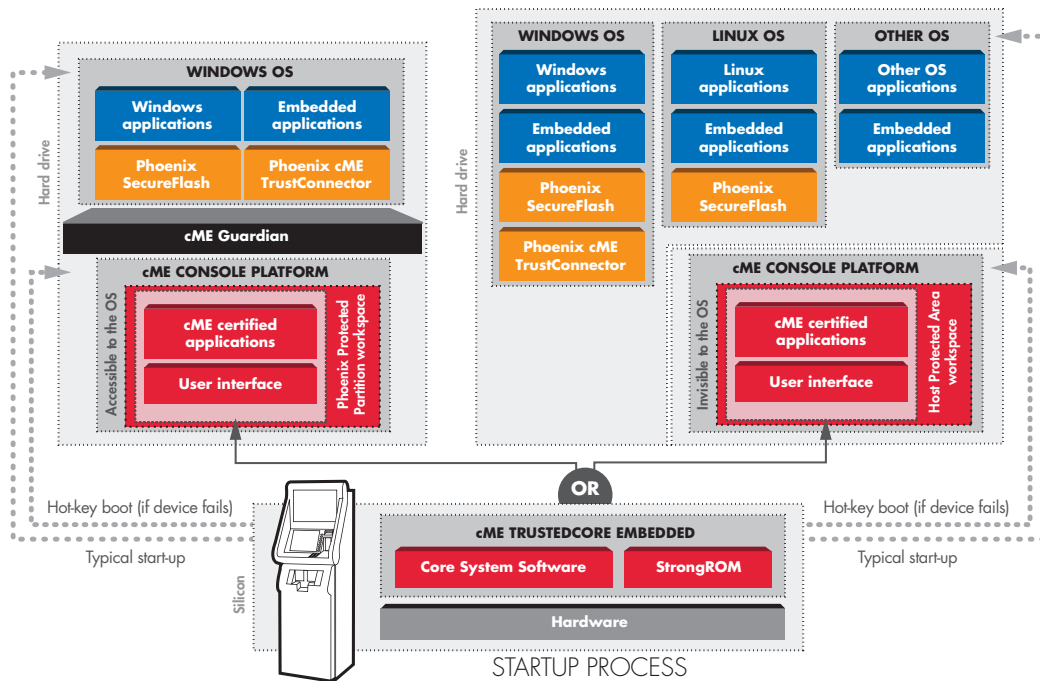
Standards

- Industry-standard x86 architecture
- Windows, Linux, proprietary, and real-time operating systems
- A complete set of industry standard technologies (please visit the Phoenix Web site for the current list of supported technologies <http://www.phoenix.com/embtechspec>)
- Intelligent Platform Management Interface (IPMI) for remote management
- Intel Extensible Firmware Interface (EFI) for preboot applications
- Microsoft Advanced Systems Format (ASF) for multimedia
- PCI, cPCI, and PCI Express for peripherals
- ATCA for wireless and telecommunications infrastructures

Developments

- Phoenix CoreArchitect for enhanced productivity during the core system software development process
- Console Platform 2004 development tools for easy custom application development and deployment
- Complete ecosystem of partners to supply motherboards, components, and specialized programming

Phoenix TrustedCore™ Embedded



Please note: The host protected area is the most secure implementation of the Phoenix cME Console because it is invisible to the operating system and defended by the firmware and the hard drive, regardless of the operating system. The Phoenix Protected Partition is slightly less secure, except in Windows environments when it is defended by the Guardian firewall.

For the latest technical specifications visit us at www.phoenix.com/trustedcore_embedded_overview

Phoenix @ the Core

Phoenix Technologies develops a complete product suite of Core System Software, tools and applications to deliver trusted, seamless computing to digital devices for an Internet-connected world. Phoenix Technologies helped launch the PC industry over 25 years ago. Today we are extending our leadership and knowledge at the core of machines, beyond the PC to a wide range of platforms and devices.

Phoenix Technologies Ltd.

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

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

