



Secure from the **START**

Phoenix
TrustedCore™
Preboot Authentication

Multi-factor authentication endpoint security via firmware

Authenticates user and device identity before the computer boots up

Manages and consolidates pre-boot user authentication

Integrates with the PBA Biometric Agent and BioTrust ID

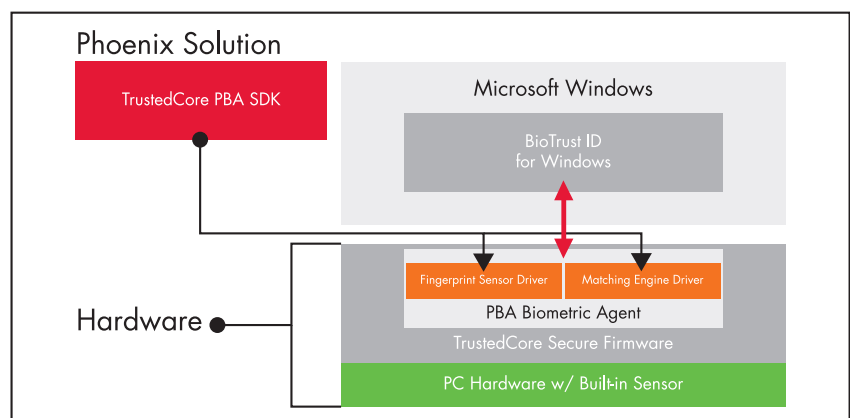
Provides fingerprint enrollment and fingerprint authentication credentials

Safer security than using general passwords

Multi-factor authentication via TrustedCore Preboot Authentication

TrustedCore™ Preboot Authentication (PBA) is a new modular architecture from Phoenix for PC security that requires a user to authenticate identity before the computer boots up. TrustedCore PBA also enables user authentication from core system software (also known as BIOS or firmware) to the operating system directly, through the BioTrust ID solution, to achieve Single Sign-On into Windows® O/S environment. The BioTrust™ ID Windows application integrates with the PBA Biometric Agent (which is an abstraction layer) through a proprietary API interface, to provide fingerprint enrollment and fingerprint authentication credentials.

TrustedCore PBA manages and consolidates, through a USB bus, various types of pre-boot user authentication mechanisms and devices, such as ASCII password, SafeNet iKey 1000 smart token, and biometric fingerprint sensors. It is a safer form of security than relying on general passwords, because fingerprint and the SafeNet ikey1000 smart token are harder to spoof or copy than general passwords.



TrustedCore PBA solution consists of TrustedCore™ SP2 or later version firmware and PBA Biometric Agent (optional module) which interfaces with vendor sensor drivers and matching engine drivers that are created from TrustedCore PBA software development kit (PBA SDK). The PBA SDK uses Microsoft MASM 6.11® or MASM 8.0 assembly language, or uses Microsoft Visual Studio .NET 2003® (or later) C language. Vendors may choose to modify the supplied Visual Studio project to make use of Microsoft Visual Studio 6.0®.



TrustedCore PBA solution requirements include the following:

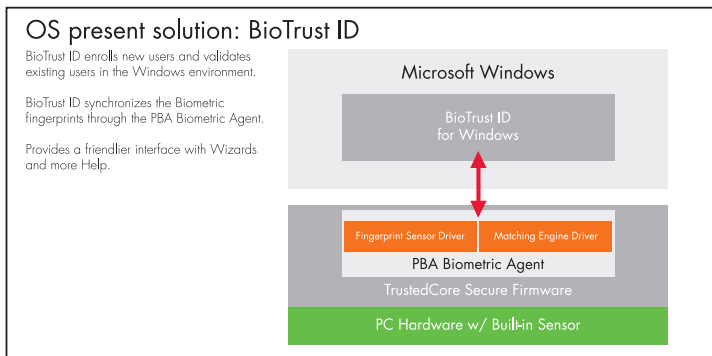
- Windows XP, Windows 2000, or Windows Vista supported
- TrustedCore SP2 source code or newer version {comes with GUI Startup Screen support and SafeNet iKey 1000 USB-based smart token support}
- PBA Biometric Agent module (optional product)
- Sufficient space for ESCD/Parameter-block of NVRAM flash memory; for example 8Mbit NVRAM supports BIOS and three reference fingerprint templates
- Driver support: AuthenTec fingerprint driver with Fujitsu Matching Engine, Validity fingerprint driver with Cogent Matching Engine
- Additional fingerprint drivers expected include FMA, Lightnning and so forth.
- Additional matching engine drivers expected include Startek and so forth.

PBA SDK includes the following in C language:

- PBA SDK device sample code and matching engine sample code
- PBA Biometric Agent binary file format to verify fingerprint driver
- Hardware reference board(s) supported (currently Intel Grantsdale board)
- TrustedCore SP2 or later BIOS Source code with one chipset module for the target development reference board
- Phoenix CoreArchitect™ 2 1-seat license
- Pre-defined hours of support from customer colutions engineering team
- Technical reference manuals for PBA SDK

A user enrolls user credentials within a target system in the following ways:

- For Smart-token devices, user enrollment is performed at the core system software level using the system’s Startup Screen menu.
- For fingerprint sensors, security enrollment is performed at the operating system level. BioTrust ID performs all requirements to enroll the user credentials and fingerprint templates for use by PBA.



Secure from the START

Phoenix Technologies is a global market leader in device-defining software that enables endpoint security from the start. The company first established dominant industry leadership over 25 years ago with BIOS software. From this unique foundation of core level expertise and firmware offering the highest levels of reliability, Phoenix has created a portfolio of innovative software products that simply and easily identify and restore devices, thereby assuring users unparalleled endpoint security and availability.

Phoenix Technologies Ltd.
 915 Murphy Ranch Road
 Milpitas, CA 95035 USA
 408.570.1000 main
 408.570.1001 fax

www.phoenix.com/trustedcore
 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.

Multi-factor strong authentication benefits include the following:

- ASCII password
- SafeNet iKey 1000 smart token
- Biometric fingerprint sensor
- Reduced time to market
- Lower development cost
- Modular architecture
- Leverage investment in TrustedCore and StrongROM and USB
- Private and tamper-resistant
- Single sign-on from firmware to Windows when combined with BioTrust ID

TrustedCore PBA solution components for OEM/ODM include the following:

- TrustedCore SP2 or later version source code
- PBA Biometric Agent module (separate product)
- BioTrust ID

TrustedCore PBA solution components for sensor-driver vendor and matching-engine vendor include the following:

- TrustedCore PBA software development kit (PBA SDK) in C language
- BioTrust ID

