

FAQ

Phoenix  
TrustedConnector™ 2

**Secure** from the START

FAQ TrustedConnector 2



Q. What is Phoenix TrustConnector 2?

A. Phoenix TrustConnector 2 is device identity software for Microsoft Windows' systems. TrustConnector 2 resolves a critical security vulnerability existing in an enterprise's security framework. It assures that the devices using a network (PC's used by employees, remote employees, partners, and customers) can be uniquely identified so that device- access privileges can be verified. Without TrustConnector 2, an enterprise network, applications, and data are vulnerable to risks created by unknown, unmanaged, or unauthenticated devices.

Q. Our organization relies on user authentication for network access. Isn't that enough?

A. No. User authentication is not enough. Every time a connection is made to your network, there are really two entities at the endpoint: the user and the device used to access the network. Consequently, it's imperative to know both your users and your devices. TrustConnector 2 creates a unique device identity that cannot be altered or stolen. It not only safeguards your business against credential sharing and stealing, but also limits access only to devices which you have granted access permission.

Q. What specific threats can Phoenix TrustConnector 2 help to prevent?

A. A single weak link of security can expose an entire network to theft or damage. By protecting both the user and device identity, Phoenix TrustConnector 2 helps protect the network. A user can be associated with a specific device or group of devices, protecting his or her identity with secure silicon in that device. If users try to access a network with any other devices, they will not have access. This helps an organization manage a device-specific security policy and prohibits unknown devices.

Q. How does TrustConnector 2 work?

A. TrustConnector 2 significantly enhances the security of digital credentials to protect against identity theft and improve security for networks and applications that use certificate-based authentication. When a Windows user or device receives a digital certificate, TrustConnector 2 re-directs the private key for that certificate out of the Windows registry where the keys are normally stored -into a secure container protected by TrustConnector. This binds the digital certificate to the computer so that the certificates cannot be stolen or moved to a different computer. The digital certificate is now unique to that computer and provides strong device identification, which in turn enables the device to be authenticated when accessing network resources.

Q. How does TrustConnector 2 protect private keys?

A. TrustConnector 2 protects private keys by creating a unique device key and using it to encrypt the private key. The device key is stored in a secure memory location on the device and cannot be removed or accessed by any software application other than TrustConnector 2. -In this way, the device key provides a unique digital identity for the device and provides the mechanism for binding the private keys (and their associated certificates) to the device.

Q. Does TrustedConnector 2 require Phoenix BIOS to work?

A. No. TrustedConnector 2 works with any PC in an installed base whether or not the PCs are equipped with Phoenix core system software (BIOS). In fact, TrustedConnector 2 can use any of three cryptographic methods: StrongROM (the Phoenix core system software cryptographic engine), Trusted Platform Modules (TPMs) or Phoenix StrongClient (Phoenix software cryptographic engine). Phoenix TrustedConnector 2 drives security all the way from the core of the machine, up into the Windows operating system, and into the network infrastructure.

Q. How Does TrustedConnector 2 know which cryptographic method to use?

TrustedConnector 2 has built-in platform sensing technology that seeks out, and uses, the best cryptographic method and secure storage available on the computer to protect the private keys. If TrustedConnector 2 is installed on a computer that is shipped with Phoenix StrongROM enabled in the core system software, it will use StrongROM and secure silicon on the motherboard to store the encrypted keys. If the device is equipped with a Trusted Platform Module (TPM) that has been enabled with the proper software components, TrustedConnector 2 will use the TPM for private key protection. If neither is found on the device, then TrustedConnector 2 will use the Phoenix StrongClient software-based cryptographic engine to protect private keys.

Q. My company is upgrading to computers equipped with a Trusted Platform Module. Can I still use TrustedConnector 2?

A. Yes. TrustedConnector 2 automatically senses whether the computer is equipped with a properly configured TPM. If there is no TPM, TrustedConnector 2 can use Phoenix StrongROM in core system software or Phoenix StrongClient software cryptographic engine. TrustedConnector 2 is an extremely cost-efficient solution, because it allows an organization to deploy a single device identity solution to all of the computers in an organization's installed base, not just the computers with TPMs.

Q. Does TrustedConnector 2 use device characteristics to create a device key?

A. No. The device key is created using standard key generating algorithms in the cryptographic engine. However when working in StrongClient mode, TrustedConnector 2 divides the key into shares and uses the device characteristics (hard drive information, component serial numbers, and so forth.) to encrypt each share separately so that it is bound to that device.

Q. How does TrustedConnector 2 plug into Windows?

A. TrustedConnector 2 provides a Windows-compatible cryptographic service provider (CSP). In turn, the CSP plugs into the standard Windows Crypto API which allows any standard Windows security-aware application to use TrustedConnector 2 and take advantage of its superior security features.

- Q. Does this mean that Windows has a built-in CSP and TrustConnector is available as a replacement for it?
- A. Yes. Windows ships with a default CSP, which stores keys in the Windows Registry. Phoenix TrustConnector 2 does not replace the Windows CSP; it provides an alternative, leaving the default CSP intact. If platform users want to improve their identity protection when they get a new digital certificate, they select Phoenix TrustConnector instead of the default Microsoft CSP. That re-directs keys out of the Windows registry into containers protected by TrustConnector 2.
- Q. Do I need a digital certificate to use Phoenix TrustConnector 2?
- A. Yes. TrustConnector 2 protects digital certificates in a public key infrastructure (PKI) from being stolen or moved from the computer to which it has been issued. Most Windows security-aware applications and network infrastructures use digital certificates for advanced security implementations.
- Q. What are some “security-aware applications” that would use Phoenix TrustConnector 2?
- A. Many standard security aware applications can use digital certificates for authentication, and TrustConnector 2 can protect those certificates. For example, you could protect the following:
- Wireless access clients, such as standard Windows XP
  - VPN access clients, such as Cisco and Checkpoint
  - Email clients for encrypted or signed email, such as Microsoft Outlook
  - Internet browsers, such as Microsoft Internet Explorer
  - Web-based business applications, such as Salesforce.com, Oracle, or SAP.
- Q. Can users opt-in (or opt-out) of any security features? Is privacy still protected?
- A. Neither Phoenix TrustedCore nor Phoenix TrustConnector 2 ships with keys or information that could be tracked in any way. Users opt-in for protection.
- Q. Does TrustConnector 2 comply with NIST FIPS 140-2 requirements?
- A. Yes. In November 2005, TrustConnector 2 was submitted for US NIST FIPS 140-2 Level 1 certification.

### **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

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.

