

Secure from the **START**

Joint Solution: **Arcot Systems**



Layered Security for Financial Institutions User Authentication and Strong Device Authentication

Strong, layered authentication is becoming a requirement for completing even simple transactions at many web portals. Implementing this high level of security has sometimes involved the use of hardware tokens – but has proven an expensive and complex rollout. Now a joint solution from Phoenix Technologies and Arcot Systems allows organizations to provide hardware- strength, layered authentication without hardware tokens. Financial institutions can now deploy robust multi-factor user authentication combined with strong device authentication – completely in software – effectively and economically.

Importance of Strong Layered Authentication

Unauthorized access costs organizations billions of dollars annually due to damages from fraudulent transactions, stolen trade secrets, litigation, private information theft, network disruption, and tarnished reputations.

In response, the Federal Financial Institutions Examination Council's (FFIEC) issued a guidance document directing that the agencies must consider "single-factor authentication... to be inadequate for high risk-transaction". Financial institutions are now required to evaluate and "...implement multifactor authentication, layered security or other controls..."

Traditional methods have significant weaknesses:

- Hardware tokens, although conceptually effective, have proven to be difficult to issue and manage for distributed consumer populations
- Software based private key containers can usually be compromised with brute force attacks
- Inability to simultaneously authenticate the user and the device he is using

Device Authentication from Phoenix

Organizations striving to strengthen authentication now have an alternative to deploying hardware tokens. Phoenix TrustConnector™ is an easy to deploy and cost effective solution that provides strong device authentication, thus ensuring that only PCs (or other devices) belonging to, or trusted by the organization can connect to the network.

TrustConnector securely and uniquely identifies individual devices during authentication, thus preventing unauthorized access - even if the attacker has managed to steal or capture valid user IDs, passwords, one-time passcodes, or digital certificates and keys. Because only authorized devices are allowed to connect, intruders and attackers are kept at bay.

ArcotID from Arcot

The ArcotID offers unique digital identity protection, providing strong user authentication and digital signing in a software form factor that works across applications and environments. The ArcotID is easy to deploy and manage, and significantly more cost-effective than hardware alternatives.

The ArcotID is based on an innovative and patented new approach known as Cryptographic Camouflage. This approach uses standard encryption algorithms in unique ways to camouflage the PKI private key and secure it against "brute force" and similar attacks.

The ArcotID presents a friendly username/password like interface to the user while appearing like a smart card to the application. This allows the ArcotID to coexist with smart cards within an enterprise.



Joint Solution: Arcot Systems

TrustConnector Device Authentication

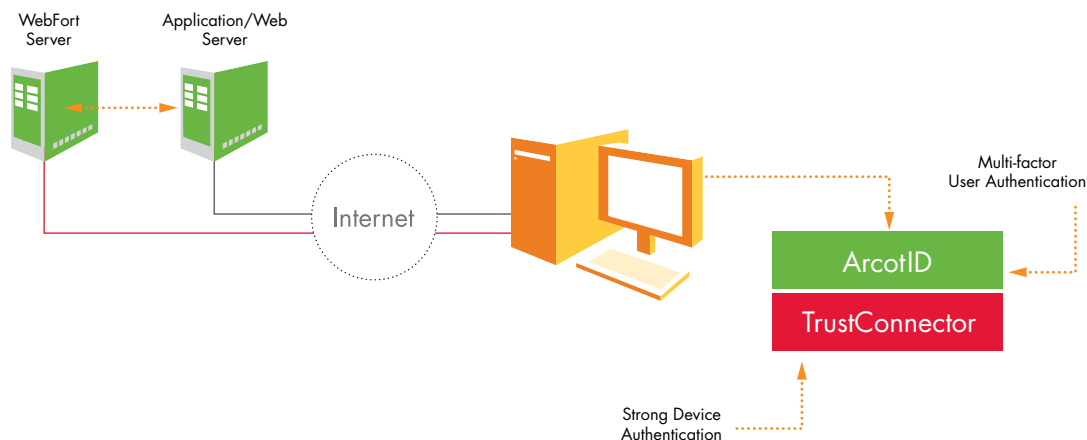
- Allows enforcement of a device-specific security policy
- Provides strong, tamper-resistant storage of user credentials
- Seamless integration with Arcot
- Easy to deploy and manage
- Installs on new or existing machines
- Delivers the promise of trusted computing today!

TrustConnector Advantage: Hardware Security

To establish device authentication, TrustConnector generates a unique device key bound to the PC's BIOS and hardware attributes. Since this works directly with the BIOS, the unique device cannot be duplicated or compromised – offering very high hardware security.

Arcot ArcotID and WebFort

- "Smart card" level security in software - tamper resistant
- Secure, digital signatures for non-repudiation
- Multi-factor user authentication to achieve FFIEC, SOX, and HIPAA compliance
- Scalable to accommodate large user communities
- Self service provisioning and reset
- Easily integrated into Web applications with the look-and-feel of a built-in security feature of the website
- Supports industry standards and easily integrates with leading certificate authorities
- The convenience of a software-only solution that supports both stationary and highly mobile users with the same user interface



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.