



ArcotID

Strong Protection for Digital IDs,
Delivered as a 100% Software-Based Smart card



PRODUCT OVERVIEW

A 100% software-based solution that provides strong protection of digital IDs for multi-factor authentication, digital signatures, and encryption.

VALUE TO CUSTOMERS

Move beyond simple username/password protection to strong user authentication and digital ID protection with a solution that is readily deployable to both internal and external users.

BRUTE FORCE ATTACK

The major operating systems store digital IDs on the hard drive and use standard encryption to protect them, controlling access with a password. If the digital ID file is stolen, standard encryption is vulnerable to an automated attack where all possible passwords are entered. Eventually this "brute force" approach will identify the correct password and allow the digital ID to be used fraudulently.

CONDUCTING BUSINESS IN AN ELECTRONIC WORLD

Organizations around the world increasingly conduct business electronically using web portals, virtual private networks (VPNs), email, and electronic documents. Electronic processes and documents, however, heighten the risk of exposing confidential information, or that fraudulent information or approvals are acted upon as though they were legitimate. Yet, most organizations require only a user name and password to access online applications. Similarly electronic documents lack a consistent method for determining if they are fraudulent or if their contents have been modified.

Threatened by increasingly sophisticated electronic attacks, organizations are moving to multi-factor authentication to decrease the possibility of fraudulent online access. Government bodies have begun to mandate that financial services institutions move beyond username/password combinations for online access or high-value transactions. In addition, organizations have begun replacing "print and sign" approval processes with digital signatures, to verify both the authenticity of a signer's identity and the integrity of a document's content.

PROTECTING DIGITAL IDS

Multiple-factor authentication, is typically based on "something you know" (e.g. password / PIN), and "something you have" (e.g. a digital ID or a One Time Password (OTP) generator) or "something you are" (e.g. fingerprint, iris scan, voiceprint, or other biometric factor). Both OTP and biometric solutions are limited to user authentication, but solutions based on digital IDs can be used for both strong authentication and digital signing.

An individual's digital ID, also known as an identity certificate or credential, is a key enabler of both strong multi-factor authentication and digital signatures. The digital ID "proves" a user's identity to applications and enables the user to apply a digital signature in place of a handwritten ink signature. The digital ID is a powerful but potentially vulnerable file – if it is ever stolen or accessed by another person, that individual can electronically impersonate the rightful owner.

The major operating systems protect digital IDs with standard encryption and a password. However, if the OS encrypted digital ID is stolen, it is vulnerable to a "brute force" attacks which will eventually reveal the correct password. Because of this vulnerability, organizations have typically protected important digital IDs in hardware such as smart cards or specialized USB security tokens.

Organizations often choose to deploy smart cards because they require not just strong authentication and/or digital signing, but they may also need to enable facility access. However, deploying smart cards and other security tokens comes at a cost of both time and complexity: smart cards and tokens must be physically distributed to users, can be lost or stolen, and require replacement and maintenance. Additionally, smart cards and tokens need driver software installed on each desktop PC – often a significant hurdle for organizations with 'locked' PC images and/or non-employee users, such as customers and partners.

ArcotID: STRONG, PATENTED SECURITY

The ArcotID®: a 100% software-based solution for protecting digital IDs against "brute force" and other types of attacks on a digital ID. The ArcotID is a configurable solution that bridges the gap between simple but insecure username/password authentication, and expensive, difficult to deploy, but very secure smart card and USB token solutions. ArcotID protected digital IDs can also be used to apply digital signatures having the same legal force as a handwritten signature, when deployed in accordance with digital signature legislation.

The Arcot "software smart card" is based on industry standards and Arcot's patented "Cryptographic Camouflage" technology to provide software-only, strong authentication that is protected against "brute force attacks".

- **Only the correct PIN/password can access an ArcotID**
- **A plausible response is generated for every PIN entered**, preventing offline identification of the PIN
- **ArcotIDs can only be used online**; must connect to Arcot® WebFort® authentication server to validate PIN
- **Repeated incorrect PIN entries lock out ArcotID**, after a WebFort configured number of failures
- **Protects against "Man-in-the-Middle" attacks**, only communicates with domain that issued ArcotID

CRYPTOGRAPHIC CAMOUFLAGE

“Since the invention of public key cryptography twenty-five years ago, people have been struggling to secure the private key without the assistance of hardware.

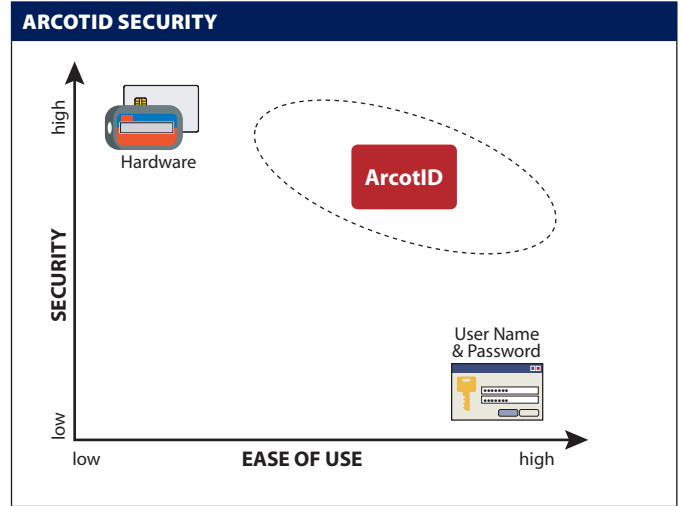
Arcot’s innovative Cryptographic Camouflage has solved this problem. Finally there is a cost-effective and convenient means to strongly authenticate users and transactions over the Internet without the need for cumbersome hardware.”*

Martin E. Hellman
Professor Emeritus
(Inventor of PKI)
Stanford University

* patent 6,170,058

ArcotID: CONFIGURABLE FUNCTIONALITY

Organizations have an array of requirements for security, ranging from situations requiring less security but demanding the simplicity of username/ password combinations, and other situations needing very strong security, typically involving smart cards and USB security tokens. ArcotIDs offer strong security, and simplicity, both ensuring the safety and security of digital IDs on the user’s computing device, and insulating the user from the underlying security technologies to make security a user friendly experience.



ArcotID AT A GLANCE

The ArcotID can be configured to match its security and usability features with the various user profiles supported by the organization.

	No Client Software	Java Applet	Light Client	Standard Client
USER CONVENIENCE				
- No install or user interaction to enable	✓			
- One mouse click in browser to enable		✓		
- Desktop install by user			✓	
- Desktop install by administrator				✓
- ArcotID On Demand Roaming	✓	✓	✓	✓
- ArcotID on Desktop / Removable (USB, CD)		✓	✓	✓
AUTHENTICATION				
- PIN/Password Never Sent Back to Server	✓	✓	✓	✓
- PIN/Password Never Stored Anywhere	✓	✓	✓	✓
- Web Applications/Portals	✓	✓	✓	✓
- Virtual Private Networks (VPNs)			✓	✓
- One Time Password (OTP) Mode			✓	✓
- HTTP Client Authentication			✓	✓
- SSL Client Authentication (MS IE)				✓
DIGITAL SIGNING & ENCRYPTION				
- Sign Web Forms	✓	✓	✓	✓
- Sign Adobe PDF, Thunderbird (email), (any PKCS#11 enabled application)			✓	✓
- Encrypt or Decrypt Adobe PDF (any PKCS#11 enabled application)			✓	✓
- Sign MS Outlook email (any CSP application)				✓
DEVICE LOCKED (ARCOTID TIED TO A SINGLE COMPUTER)				
- Processor Type & Processor Serial Number (PSN only available on some CPUs)				✓
- Hard Drive Volume Serial Number (VSN)				✓
- Network Adapter MAC Hardware Address				✓
- BIOS (through Phoenix TrustConnector)				✓



Clientless and Optional Client Functionality

Organizations can deploy the ArcotID with several client options, ranging from no client to a full native client, that offer different levels of security, capability, and convenience. Each offers different levels of security, convenience, and capabilities. ArcotID can provide protection from the following attack types: “brute force”, “man-in-the-middle”, “keyboard logging”, “mouseclick logging”, and “phishing”. The degree of user interaction and administration rights required to configure an ArcotID vary depending on the client selected.

ArcotIDs are supported on multiple PC operating systems providing instant access to critical data when and where users need it, while keeping online resources safe from unauthorized access.

On Demand Roaming Access

The ArcotID can be stored locally on a desktop computer or removable media (USB Flash drive, CD-ROM, floppy disk, etc). It can also be downloaded On Demand from the Arcot WebFort authentication server for a consumer user that requires complete transparency from multiple computers, by a user who has misplaced their hardware token, or for a temporary user such as a visiting physician or contractor needing temporary electronic access.

Risk-Based Authentication

Authentication to different classes of applications can be supported depending on the client option selected by an organization. For example, in high volume consumer deployments the organization can choose the option requiring no client software, so the consumer will continue to authenticate with a simple username/PIN. A fully installed ArcotID client is only required when authenticating to non-web-based applications – more typical in certain enterprise or government environments.

An additional strength of the ArcotID is that the user’s PIN/password is not stored on any server or ever transmitted over the network. This means a customer can safely use the same PIN/password with any organization deploying ArcotIDs without having to worry that a security breach to one organization will compromise access to information or accounts at other organizations.

The ArcotID authentication solution can be made even stronger by coupling it with Arcot RiskFort, to perform risk analysis on each authentication attempt. See the Arcot RiskFort datasheet for more information.

Device Locked Authentication

An ArcotID can be locked so it functions only on a specific computer. Arcot accomplishes this by incorporating hardware information into the encryption routines used to initially create the ArcotID, which become part the PIN used to access it. The ArcotID is then rendered useless if is taken to another computer.

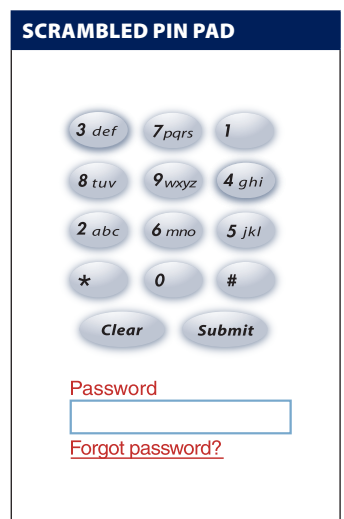
Scrambled PIN Pad

The ArcotID can help protect users against keystroke logging and mouse click logging malware/crimeware that may be installed on a computer. Logging crimeware captures every keystroke and mouse click on the computer and periodically sends that information over the internet to the criminal or hacker who created it. Arcot’s patented* scrambled PIN Pad thwarts logging malware: users enter their PIN by clicking with a mouse on a screen-based PIN Pad that changes the number locations either once or after every mouse click as configured by the organization. The scrambled PIN PAD is an option that can be used in any of the ArcotID clients.

Digital Signing and Encryption

Once a user has been provisioned with an ArcotID, they can easily add Digital IDs (identity certificates) into the ArcotID to enable digital signing and/or data encryption. Replacing “print and sign” with digital signatures on electronic documents enables fully electronic business processes while maintaining legal enforceability, validates that the correct individual approved a document, and provides easy detection of unauthorized changes.

Additionally, the ArcotID’s encryption capabilities enable organizations to send confidential information via email that can be opened only by authorized recipients. Unlike many other “specialized” solutions, the ArcotID user authentication experience is identical to how the recipients access the sending organization’s web site. Many organizations want to email monthly bills, explanation of medical benefits, and other financial information, so that they replicate the “push” model currently used with paper documents, but also comply with government privacy regulations. The ArcotID solution makes it easy to move to a secure electronic push distribution model, even for sensitive documents.



DESKTOP PLATFORMS

BROWSERS

- MS Internet Explorer
- Firefox
- Mozilla
- Netscape Navigator
- Apple Safari

CLIENT PLATFORMS

- Microsoft Windows (98, 2000, 2003, XP)
- Sun Solaris
- Mac OS X
- Linux

ArcotID FEATURES AND BENEFITS

FEATURE	BENEFIT
Requires no additional hardware	<i>Reduces initial cost, complexity and deployment time versus hardware solutions; eliminates ongoing hardware maintenance/support.</i>
Supports “zero footprint” on desktop	<i>Easy to provision and support even on locked desktops for internal or external users because no software installation is required</i>
Protects digital IDs with Arcot’s patented Cryptographic Camouflage technology	<i>Resists “brute force” and “man-in-the-middle” hacker attacks</i>
Transparent user experience	<i>Appears to user as password authentication; no user retraining required</i>
On Demand download of ArcotID	<i>Enable users to authenticate from any computer to support consumer anytime, anywhere access</i>
Temporary credentials	<i>Easily issue (and revoke) credentials for temporary or remote users</i>
Support for challenge/response, one time password, and username/password authentication models	<i>Eases the migration process from username/password to strong authentication.</i>
Scrambled PIN Pad	<i>Protects against keystroke and mouseclick loggers</i>
Device Locked	<i>ArcotID is usable only from a single computer for higher security</i>

STRONG SECURITY WITH THE SIMPLICITY OF A PASSWORD

The ArcotID overcomes two critical challenges for organizations wishing to improve the security of their electronic systems:

- Ensuring safety and security of digital IDs on the user’s computing device
- Making increased security user-friendly by insulating the user from the underlying security algorithms and technologies.

THE ArcotID IN ACTION

Arcot customers have deployed the ArcotID to increase security for the following applications:

- Replace weak passwords with strong multi-factor authentication for secure VPN or Partner Portal access
- Provide secure web mail access
- Apply digital signatures to critical documents
- Provide temporary credentials to partners or customers
- Provide strong authentication for the extended Enterprise

As a result of its deployment and configuration flexibility, cost savings, and security, Arcot has emerged as the leading provider of software-based strong authentication solutions for large scale deployments of strong authentication and digital signature applications.

ABOUT ARCOT SYSTEMS

Arcot is a leading provider of strong two-factor authentication and digital signature solutions. Arcot’s software offerings are compliant with industry standards including 3-D Secure, IdenTrust, and SAFE. Over 10,000 banks and other enterprises use Arcot to protect the identities of millions of employees, partners, and consumers worldwide. Organizations also work with Arcot to comply with regulations or legislation such as FFIEC, Sarbanes-Oxley, and HIPAA. Visit www.arcot.com.



Corporate Headquarters | Arcot Systems, Inc. | 455 West Maude Avenue | Sunnyvale, CA 94085-3517 USA | www.arcot.com | (408) 969-6100
Arcot International | Trinity Court-A | Wokingham Road | Bracknell, Berkshire | RG42 1PL UK | +44 01344 668 280
Arcot Deutschland GmbH | Schulweg 7 | D-82343 Pöcking | Munich, Germany | +49 8157 997793

Arcot, the Arcot logo, ArcotID, Arcot KeyFort, Arcot RegFort, Arcot RiskFort, Arcot SignFort, Arcot TransFort, Arcot TrustFort, Arcot WebFort, Arcot Universal SAFE Signing Interface, and Arcot Universal Client, are trademarks or registered trademarks of Arcot Systems, Inc. in the United States and other countries. Other trademarks are the property of their respective owners.