ARCOT®

Strong Authentication for Secure VPN Access

Solving the Challenge of Simple and Secure Remote Access

WHITEPAPER

EXECUTIVE SUMMARY

In today's competitive and efficiency-driven climate, organizations must provide their employees, contractors, and business partners with secure remote access. Many organizations provide access via a Virtual Private Network (VPN) over existing internet connections.

However, VPNs solve only part of the security equation for remote access. VPNs ensure the privacy of data transmission, but do not strongly defend against unauthorized access to the organization's electronic assets. Today, simple username and passwords protect access to most VPNs.

Security experts recommend strong, two-factor authentication to protect remote access. However, strong authentication historically has been expensive, difficult to use, and complex to administer. This has left organizations with a dilemma — take on the added expense and burden of two-factor authentication or leave the organization's remote access inadequately protected.

Arcot Systems Inc., a leader in software-based strong authentication and digital signing solutions, provides a third option for secure remote access: strong two-factor authentication for VPNs that retains the ease-of-use and deployment simplicity of username/password authentication.

Remote Access Is Vital To Business Today

Doing business today means doing business over the internet. Employees, contractors, and business partners want access to the information they need, where and when they need it.

Many organizations use virtual Private Networks (VPNs) to provide secure access to their electronic resources. VPNs create a private "tunnel" through the public internet between a remote user and the organization's internal network. The VPN encrypts the data in the tunnel, preventing anyone who intercepts the data from being able to understand the contents. VPNs enable users to gain access to a company's internal network from anywhere in the world, through a range of methods:

- *Simple web-based interfaces* that allow secure, authenticated access to web applications such as a partner portal
- *Full client deployments* that provide a "virtual office" with file sharing, print sharing, and legacy application access for remote users
- *Dedicated links* that connect branch offices to corporate headquarters

"First Mile" Insecurity Leaves Data At Risk

Although the tunnel created by the VPN keeps information that flows through it private, it does not prevent unauthorized access to the organization's network. Often, there is nothing more than a simple username and password protecting the "first mile" of a VPN, the connection to the client PC. Attacks such as Man-In-The-Middle (MITM), brute force and Spyware can compromise passwords.1 Once they compromise login credentials, attackers can gain access to the organization's internal network.

To reduce the risk of compromise, most security experts recommend the replacement of simple username/password combinations for online access authentication with stronger authentication methods. Multi-factor authentication (also known as "Strong authentication") requires users to employ more than one factor to prove their identity before they receive online access. Factors can include:

- *Something you know* (such as a PIN or password);
- *Something you have* (such as a smart card, digital ID, or One Time Password generator);

- *Something you are* (a biometric factor such as fingerprint or voiceprint).

Traditional Two-Factor Security Is Costly And Complex

Moving to strong authentication can be both costly and complex. Deploying a strong second factor, (e.g., "something you have"), typically involves security hardware such as USB tokens, smart cards, or one-time password (OTP) tokens. These hardware solutions can be cost-prohibitive for an organization due to the following reasons:

- *Direct and indirect costs* to manage and distribute security hardware
- *Periodic replacement of OTP tokens* due to battery failure
- *IT configuration changes* to install drivers on PC desktops with locked, standardized configurations
- *Replacing and distributing* lost or broken security hardware

In addition to the costs described above, traditional two-factor solutions introduce additional complexity to both the user and the IT infrastructure, especially when provisioning security hardware for business partners. This complexity consists of two major issues:

- *Users managing multiple security tokens with different user interfaces.* Studies have shown that users will attempt to subvert any security deployments they believe impedes their productivity. This can translate into actions as simple as placing passwords on sticky notes or as serious as sharing tokens.
- *Business partners juggling multiple tokens from multiple partners.* Organizations must successfully deploy and support a VPN client plus an authentication solution to a business partner who may already be struggling with conflicting login processes from other organizations.

Another challenge to successful deployment of two-factor authentication for VPNs is that a strong authentication solution must meet the security needs of a full spectrum of applications. The applications range from those requiring very high levels of security, such as financial data, customer information, and product development plans, to others that may need less security, such as an internal news portal or other information site.

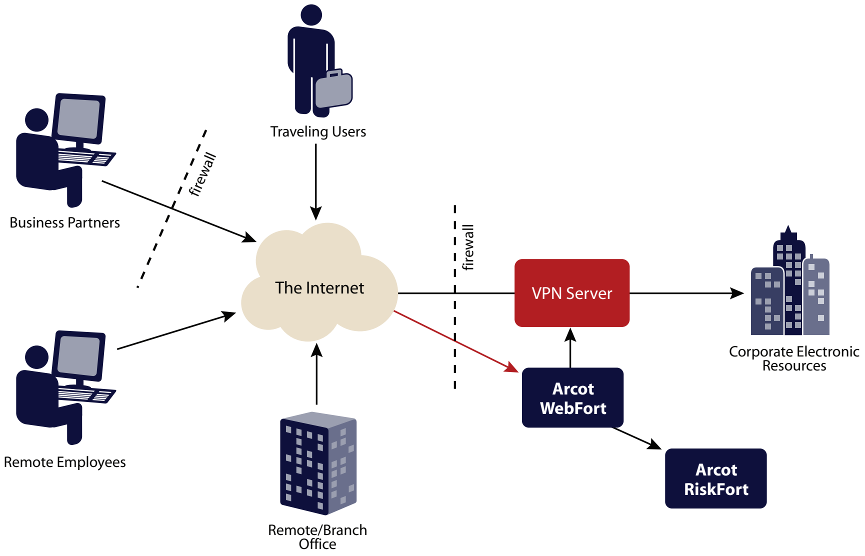
IT organizations faced with this dilemma must choose between the painful and risky options of leaving assets insufficiently protected or beginning a complex, expensive, multiyear project to provide multiple levels of authentication for the organization.

Arcot® Two-Factor Simplicity And Security

Arcot has the solution to address these challenges: the ArcotID®, a 100% software, strong authentication "software smart card." This solution has the same functionality and interoperability as a hardware smart card, yet is significantly easier and less expensive to deploy, manage, and use.

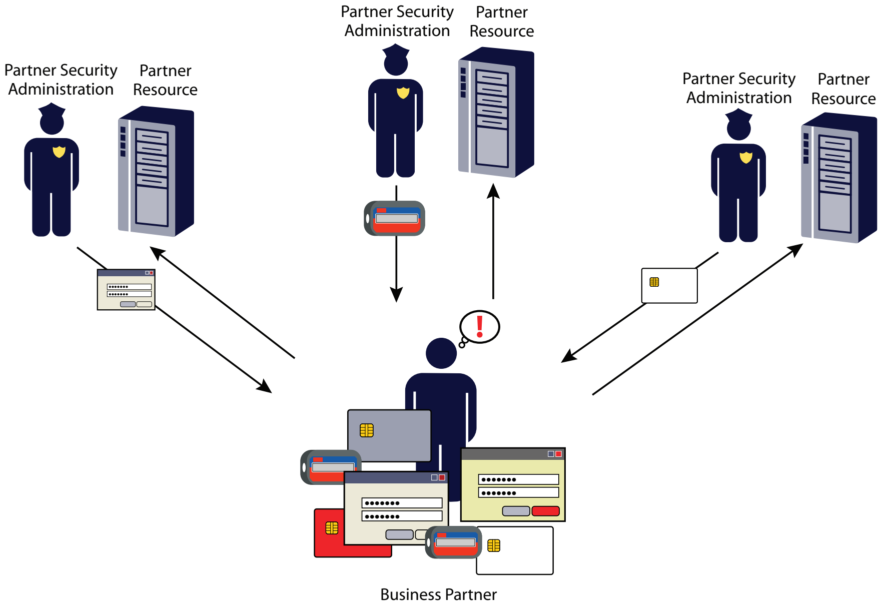
Arcot provides strong, two-factor security in the ArcotID through its patented Cryptographic Camouflage™ technology.

ARCOT SECURES VPN AUTHENTICATION FOR ALL TYPES OF USERS



A "Man-in-the-Middle" attack occurs when an attacker inserts himself in the middle of a session between a client and server, such as a remote user and a web portal. Masquerading as both the legitimate client and server, the attacker intercepts all communications including log-on credentials and one-time-password tokens. A "brute force" attack occurs when an attacker exhaustively attempts every possible password to break into a system. This type of attack is more feasible as computing hardware becomes cheaper and faster.

THE BUSINESS PARTNER'S DILEMMA – MANAGING MULTIPLE IDS AND TOKENS


Partner Security Administration
Partner Resource
Partner Security Administration
Partner Resource
Partner Security Administration
Partner Resource
Business Partner

The ArcotID is not vulnerable to MITM attacks or brute force attacks that attackers can mount against other software tokens and credential containers.

The ArcotID adds security without adding complexity. Organizations can configure the user experience to look identical to existing username/password authentication. The underlying patented Arcot technology delivers strong authentication for secure access invisibly and reliably.

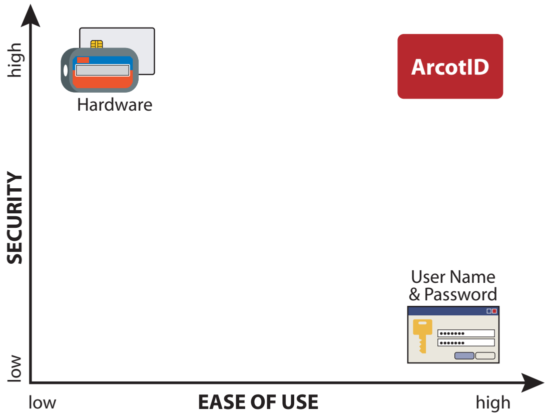
The ArcotID is easy to integrate with existing authentication solutions. It supports applications enabled for hardware smart cards or USB security tokens without any application changes. It also supports applications that enable OTPs without modification using the included RADIUS interface. In short, ArcotID allows organizations to exercise control over electronic access with no requirement for new hardware, readers, or drivers.

Arcot's software-based approach eliminates the burden of deploying and supporting hardware tokens. With its simple user interface, the ArcotID keeps support and training costs low and user adoption rates high.

FEATURE COMPARISON OF STRONG AUTHENTICATION SOLUTIONS

	USERNAME/ PASSWORD	OTP HARDWARE	SMARTCARD	O/S KEY STORAGE	ARCOTID
Multi-factor authentication (strong)		✓	✓		✓
Digital signature capable			✓	✓	✓
File encryption capable			✓	✓	✓
Man-in-middle attack resistant			✓	✓	✓
Familiar user interface	✓				✓
Brute-force resistant		✓	✓		✓
Client-less software option	✓	✓			✓
Unlimited life (no battery)	✓		✓	✓	✓

ArcotID DELIVERS THE STRENGTH OF HARDWARE WITH THE EASE OF SOFTWARE



Organizations can deploy the ArcotID more quickly than hardware smart cards and OTP tokens. Arcot's fully self-service web provisioning system can provision ArcotID software smart cards to employees and partners with zero administrator assistance. Existing desktops do not need additional software nor do they need any new hardware to deploy an ArcotID.

These features enable substantial cost savings for the organization:

- Online self-enrollment
- Lost credential recovery
- Fast temporary credentials issuance
- Location-dependent access controls
- No end-user software install
- Support for roaming access

Take Control Over The Authentication Lifecycle

Arcot VPN authentication solutions are part of Arcot's family of authentication products that address the needs of the entire authentication lifecycle, from issuing credentials, to risk management and revocation.

Arcot RegFort™ enables organizations to choose from a range of options for distributing authentication credentials. They can allow full self-service or IT-directed operation with multiple registration capabilities for additional control. RegFort also supports loading digital IDs into ArcotIDs or hardware smart cards to provide additional flexibility for IPSec-based VPNs, client SSL certificates and other digital ID-enabled applications.

Arcot WebFort® is a high performance authentication server that supports both password and strong two-factor authentication using the ArcotID to provide a fully software-based strong authentication solution. WebFort even supports a mixture of strong authentication and username/password infrastructures mode deployments.

To enhance the authentication process further, Arcot RiskFort™ offers sophisticated real-time risk management. RiskFort derives a risk score by evaluating aspects of each online transaction. It examines data points such as the originating device, the geographic location of the user and the nature of the authentication event, and then correlates these aspects with user behaviors. RiskFort uses this to detect and block potential malicious activity automatically before it can do any damage.

A simple, consistent user experience

Arcot delivers a comprehensive, strong authentication solution for all the major enterprise VPN technologies including SSL, Hybrid or Tunneling SSL and IPSec-based VPNs. Arcot's patented Cryptographic Camouflage™ technology protects all remote users. Regardless of the VPN technology used, authentication using an ArcotID is a simple and intuitive process. A user with an ArcotID initiates a connection to the organization's VPN and performs one of two familiar tasks when prompted:

1. Enter a username

2. Enter a PIN/password

Ease of use and a consistent login experience are critical to the success of a secure authentication deployment. ArcotID provides both.

RELATIVE COSTS OF STRONG AUTHENTICATION SOLUTIONS

	OTP HARDWARE	SMARTCARD	ARCOTID
Direct cost (including reader)	$ $ $ $	$ $ $ $ $	$ $
Shipping cost	$ $	$ $	–
Replacement cost	$ $	$ $	–
Training cost	$ $	$ $	$

Conclusion

Organizations must provide secure remote access to their employees, contractors and partners in order to remain competitive in the marketplace. VPNs provide a reliable way to secure the data transmission for remote access, but do not address the security of the login process itself. This insecurity leaves the entire network at risk.

In the past, organizations have faced a difficult choice between deploying complex, expensive, difficult-to-use but secure authentication technology and authentication technology that was easy, inexpensive and insecure.

Fortunately, Arcot has the solution to satisfy the need for two-way authentication for VPN users: the ArcotID, a 100% software, strong authentication "software smart card." This solution has the same functionality and interoperability as a hardware smart card, yet is significantly easier and less expensive to deploy, manage, and use.

Arcot's proven, secure authentication solutions scale to meet the size and complexity of any organization, extending the reach of organizational extranets to remote employees and business partners. Arcot protects over 11 million users while maintaining the performance and responsiveness demanded by today's authentication infrastructures.

About Arcot

Arcot is the cloud authentication leader. Our fraud prevention, strong authentication, and e-Document security solutions make Web transactions and online access safe for millions of consumer, enterprise, and e-Commerce users. Organizations can transparently deploy stronger authentication and allow users to conveniently authenticate from any computer or mobile device. Arcot solutions deliver the right balance of cost, convenience and strength.

For more information, please visit www.Arcot.com, email sales@arcot.com, or contact your nearest sales office:

Corporate Headquarters, U.S.
Arcot Systems, Inc.
Ph: +1 408 969 6100

United Kingdom
Arcot International
Ph: +44 118 965 7998

Germany
Arcot Deutschland GmbH
Ph: +49 8157 997793

India
Arcot R&D Software Private Ltd
Ph: +91 80 6660 2745

ARCOT®

www.arcot.com

10-85