



# How Arcot Solutions Protect Against Internet Threats

Whitepaper

WHITEPAPER

## OVERVIEW

Protects organizations from Man-in-the-Browser and Man-in-the-Middle attacks than can defeat other authentication technologies.

Fraud-proofs login process without changing user behavior, or requiring expensive hardware.

Provides one secure credential for multiple applications

Offered as a SaaS service or available for on-premise installation

## INTRODUCTION

Regulatory requirements are making strong authentication mandatory. Simple username and password login processes are no longer sufficient. Traditional approaches like OTP tokens are expensive to deploy and manage and are ineffective against some threats. The challenge you face is deploying a technology that is both easy to use yet strong enough to protect against sophisticated attacks like Man-in-the-Browser and Man-in-the-Middle.

Arcot offers a wide range of software-only, multifactor, and two-factor authentication solutions that transparently protect and verify your Web users' identities. Arcot Solutions protect your customers, partners, and employees from identity theft and fraud without the need to change their familiar login experience. By employing innovative, patented authentication technologies, Arcot solutions uniquely defeat attacks like man-in-the-middle and man-in-the-browser which typically evade other authentication technologies.

Basic adaptive access control including fraud monitoring, detection and prevention capabilities are provided by Arcot RiskFort™. Arcot RiskFort employs real time risk-based authentication technologies such as deviceID checking and IP Geolocation to identify legitimate users. If a user is deemed suspicious, the transaction or login can be denied or can be flagged for additional step up authentication. Arcot WebFort® provides a range of multifactor authentication options including Security Questions & Answers, OTP to mobile phone via SMS, OTP via email and the ArcotID® Secure Software Credential. WebFort also includes a Personal Assurance Message for site verification and a scrambled pin pad to protect against keystroke and mouse click loggers.

Arcot authentication solutions are offered for deployment on-premise or on-demand as an Arcot hosted service called A-OK On-Demand. You choose the deployment model to suit your environment.

This white paper describes how to prevent internet threats using WebFort with the ArcotID .

### ArcotID Security

The ArcotID is a secure software credential that combines protection for digital identities like that of a hardware smart card with ease of use, ease of distribution, and lower costs for deployment and maintenance. The ArcotID is the 'something you have' and the ArcotID password is the 'something you know' necessary for two-factor authentication. The ArcotID can reside on the local desktop, PDA, or can be carried in any persistent memory device, such as a USB memory stick. The ArcotID resists brute force attacks using patented Cryptographic Camouflage technology to protect a user's digital ID from attackers. The technology has been vetted by academics<sup>1</sup> and Fortune 500 companies.

Organizations can use the ArcotID for two-factor challenge/response-based authentication, and for securely storing extra application keys. The ArcotID can also store other user data for additional applications such as electronic document signing, secure email and e-Document delivery. As a software-based solution, the ArcotID enables organizations to leverage the advantages of Public-Key Infrastructures without the expense and management issues inherent with hardware-based secure key storage.

The ArcotID authenticates with the authentication server as follows: The authentication server first sends a hidden "challenge" (a random string of text) to the ArcotID. When the user provides the correct password to the ArcotID, the ArcotID uses the private key to sign this "challenge" to create the corresponding "response".

<sup>1</sup> See "Software Smart Cards via Cryptographic Camouflage", D.N. Hoover and B. N. Kausik, Proceedings of the 1999 IEEE Symposium on Security and Privacy, IEEE Computer Society.



Only this “response” is sent back to the authentication server for verification. The ArcotID does not store the password used to derive the private key anywhere, or transmit it to the server. By providing the challenge/response sequence in addition to multi-factor authentication, Arcot can uniquely protect businesses and customers from Man-in-the-Middle attacks.

While highly secure, the ArcotID features an easy-to-use and familiar username/password interface and integrates quickly with existing authentication infrastructures with support for standards such as RADIUS-based OTP, SAML, MS CSP and PKCS#11. This makes deployments fast and easy for an organization to implement and its customers to use.

Arcot has also developed a patented technology to protect PIN/password entry from keyboard capture attacks. This

optional Scrambled PIN-pad defeats keyboard “sniffers” by requiring the user to “click” the digits of their personal PIN on a virtual keyboard. Organizations can configure the virtual keyboard to scramble the keys after each mouse click or each password entry, thus preventing the malware from reading any keystrokes or making pattern guesses based on mouse click locations.

The ArcotID provides protection against common internet attacks and several new attacks that are becoming popular among fraudsters. Other solutions, including one-time-password (OTP) generator tokens, do not offer the same level of protection against attacks such as the man-in-the-middle attack. The following table contains a list of known threats and shows how Arcot defeats those attacks.

**THREATS AND HOW ARCOT DEFEATS THEM**

THREAT	DESCRIPTION	HOW ARCOT DEFEATS THE THREAT
<p><b>Brute Force</b></p>	<p>The attacker copies the key container to his own equipment and exhaustively attempts millions of passwords, which eventually leads to the disclosure of the private key.</p>	<p>Arcot’s patented “Cryptographic Camouflage” technology uses a password as a basis for encrypting the private key. It uses standard encryption algorithms and the patented Arcot process to protect the key. The result of this process is that any decryption attempt, including using an incorrect password, will always produce a result that meets the specific, particular, and well-documented characteristics of a private key. A six-character password will have approximately 56.8 billion permutations (upper case, lower case, and numbers), and only one of those permutations will unlock the private key.</p> <p>During the authentication process, the authentication server requires the decrypted key to generate a response by digitally signing the authentication challenge it issued.</p> <p>If the authentication fails because an incorrect key was used to generate the response, the invalid password counter increases by one. The authentication server can block user access after a configurable number of invalid attempts (the default is three) Therefore, the attacker can attempt very few passwords before being locked out.</p>
<p><b>Challenge/Response Intercept</b></p>	<p>The attacker intercepts the challenge issued by the authentication server and the signed response from the client. The attacker then uses every possible private key to recreate the signed response and discover the true private key.</p>	<p>The authentication challenge/response is sent over a secure SSL channel. Even if an attacker were able to break the channel security – which is extremely unlikely – this attack still fails because the standard signature algorithm always includes random padding to ensure the uniqueness of every signed response. Only the authorized authentication server, which has access to the corresponding public key, can verify the signature.</p>

## FEATURES AND BENEFITS

THREAT	DESCRIPTION	HOW ARCOT DEFEATS THE ATTACK
<b>Chosen Plaintext</b>	The attacker tests every possible key against a known piece of text that has been encrypted with the public key and can tell when he has discovered the true private key as it would correctly decrypt the plaintext.	The attacker will not be able to mount this attack since he does not have access to the ArcotID plain public key. In the ArcotID scheme, the public key used for authentication is encrypted by the domain root key thereby making it possible to control its release to trusted parties only.
<b>Fraudulent Administrator</b>	The attacker is a fraudulent administrator who gets access to the ArcotID on the server.	A fraudulent administrator may get access to the ArcotID, but the administrator cannot use it without the password. The password is not stored anywhere, nor does it travel to the server during authentication. It is used only to de-camouflage the private key at the client when the challenge is signed. Only the user knows his password – this feature ensures that the ArcotID offers non-repudiation.
<b>Man-in-the-Browser</b>	<p>The attacker uses malware, typically a trojan, to modify a user's transactions in real-time.</p> <p>Unlike other phishing attacks, there is no change to the URL with which the user authenticates. The attack 'piggybacks' on a legitimate session after the user has authenticated himself via single- or multi-factor authentication.</p>	<p>Arcot defeats Man-in-the-Browser by validating the integrity of the data in a transaction, as well as providing in-band authentication of the transaction itself. Arcot incorporates two unique approaches to defeating MITB attacks:</p> <p><b>Digital Signing of Forms:</b> Arcot's approach leverages the ubiquitous Adobe Reader/Acrobat client, with its embedded Arcot technology. Because the transaction occurs completely in the Adobe Reader/Acrobat environment, it is completely separate from any browser-based trojan or helper application.</p> <p>Upon initiating a transaction, the user is presented with a PDF-based form, into which he enters all transaction details. The user then submits the form, causing the Adobe client to invoke the embedded ArcotID client. The ArcotID authenticates the user and digitally signs the PDF, allowing the server to complete the transaction. The form data is never exposed to an MITB as it takes place outside of a browser environment.</p> <p><b>Virtual Private Session (VPS):</b> Arcot's patent-pending VPS creates a virtual session with the end-user. The VPS exposes any changes in the transaction made by malware in the browser, or any browser helper objects. Arcot VPS presents details of the transaction along with a Transaction Confirmation Code back to the user in a CAPTCHA format in the same web channel. This approach does not depend on alternate channels or back-end analysis. The user reads the CAPTCHA, verifies the transaction details, and enters the confirmation code to confirm the transaction within a specific time period. The MITB Trojan is unable to parse the CAPTCHA and read the Transaction Confirmation Code within the time available. If the MITB has modified the transaction, the CAPTCHA image will show the modified transaction in its entirety. The user can easily detect a change from what was originally entered and can stop the transaction and prevent the MITB attack.</p>

### FEATURES AND BENEFITS

THREAT	DESCRIPTION	HOW ARCOT DEFEATS THE ATTACK
<b>Man-in-the-Middle</b>	The attacker intercepts the credentials and data while they are in transit. In this case, the attacker appears as the target server to the user and as the user to the target server.	Each ArcotID contains information about the domain that issued it. The ArcotID client automatically checks the Arcot certificate to confirm that it is connected to the same domain before signing the challenge response. If the domains do not match, the ArcotID client will not sign the challenge and the attacker will not be able to complete the authentication.
<b>Pharming</b>	The attacker poisons the DNS server and redirects users to the fraudulent web site. Users do not suspect anything because the redirect happens even when the user selects the web site from a saved favorite or actually types in the correct URL.	As mentioned above, each ArcotID contains information on the domain that issued that ArcotID. The ArcotID client automatically checks to confirm that it is connected, via SSL, to the right domain before signing the challenge string. If the domains do not match, the ArcotID client will not sign the challenge and the attacker will not be able to complete the authentication.
<b>Phishing</b>	The attacker targets unsophisticated users and fools them into entering their credentials into a fake web site. This usually occurs when a criminal sends an email impersonating a customer service organization from a legitimate business (such as a bank or payment site) and asks recipients to click on a URL to perform account maintenance or verification. The link takes them to a fraudulent site, which prompts them for their valid credentials.	<p>One key advantage of the ArcotID's two-factor authentication is to protect users from phishing attacks. Again, assuming phishers can convince a user to disclose their password, they are still unable to impersonate the user as they don't have the second factor (the ArcotID). The phisher needs both what the user has (the ArcotID file) and what the user knows (the Password).</p> <p>Arcot also provides protection against phishing attack even when two-factor authentication is not used:</p> <ol style="list-style-type: none"> <li>1. A Risk Engine (RiskFort) to determine if the user is coming from a registered device, geographical location, or other predetermined check. The engine can recommend an out-of-band check if necessary.</li> <li>2. A shared secret that the user establishes with the application server — Personal Assurance Message (PAM). The site prompts the user for his user ID only. After the user enters his user ID, the site displays the PAM if the risk engine is confident with the checking result. The user can make sure he is not communicating to a phishing site before he enters his password.</li> </ol>
<b>Replay Attack</b>	The attacker stores a copy of the signed challenge and replays it to the site.	The Arcot authentication involves a PKI-based challenge/response model where the challenge sent to the client for signing is a freshly generated random block. When the signed challenge is sent to the server for verification, the server verifies the challenge and marks the particular signed challenge as having been verified. The uniqueness of the random challenge defeats the replay attacks.
<b>Key-Logger</b>	The attacker installs key-logging malware that captures every keystroke and mouse click on the computer and periodically sends that information over the internet to the criminal who created it.	Arcot's optional patented scrambled PIN Pad thwarts logging malware. The PIN-pad is a virtual keyboard that shows up on the screen; users enter their password by clicking with a mouse on a screen-based key pad. The user will not use the keyboard to enter the ArcotID password and is hence protected completely from keyboard loggers. The scrambled PIN pad ensures that mouse click loggers are unable to determine what keys are actually pressed by optionally changing the position sequence of the keys on the PIN-pad after every click.

## FEATURES AND BENEFITS

THREAT	DESCRIPTION	HOW ARCOT DEFEATS THE ATTACK
<b>Malware Browser Memory Attack</b>	The attacker attempts to find the private key in the memory of a system that has downloaded the ArcotID in roaming mode when the user does not close the browser (such as at a public Internet kiosk).	<p>When the ArcotID is downloaded into memory, the private key is still camouflaged – it is not in the clear. The private key appears only briefly when the challenge is signed and the user provides the password. Immediately after signing the challenge, the private key and password are cleared from memory; only the response (encrypted challenge) is sent back to the server—the ArcotID never sends the private key and password to the server.</p> <p>Even if the user does not close the browser, only the protected ArcotID may be in memory. The web page that downloaded the ArcotID can also remove it from memory by clearing the memory immediately after the authentication.</p>

## COMPARISON BETWEEN ARCOTID AND OTHER AUTHENTICATION TECHNOLOGIES

	Man-in-the-Browser	Man-in-the-Middle	Pharming	Phishing	Replay Attack	Key-Logger
ArcotID	✓	✓	✓	✓	✓	✓
OTP HW Token	—	○	—	✓	✓	○
Risk Analysis	—	○	○	—	○	○
Personal Assurance	—	○	✓	—	○	○
Virtual Keyboard	—	n/a	n/a	n/a	n/a	✓
Identifying Questions	—	○	✓	✓	✓	○
Out of Band	—	○	✓	✓	✓	○
Split Key	—	○	✓	✓	✓	○
Scratch Cards	—	○	✓	✓	○	○

## COMPARISON BETWEEN ARCOTID AND PKI BASED AUTHENTICATION

	Brute Force	Fraudulent Admin	Challenge/Response Intercept	Chosen Plaintext	Malware Browser Memory Attack
ArcotID	✓	✓	✓	✓	✓
Split Key	✓	✓	○	○	○
Client SSL Certificate	—	—	—	○	○
Plain Certificate	—	—	—	○	—

**Legend:** ✓ = Full protection; ○ = Partial protection; — = No protection

### 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](http://www.Arcot.com), email [sales@arcot.com](mailto: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



[www.arcot.com](http://www.arcot.com)

Copyright © 2010 Arcot Systems, Inc. All rights reserved. Arcot, Arcot WebFort and ArcotID are registered trademarks of Arcot Systems, Inc. All other trademarks are the property of Arcot Systems, Inc. or their respective owners.

10-147