



Arcot Customer FAQ

RiskFort & WebFort

Customer FAQ

Introduction

Arcot delivers authentication and digital signing solutions for consumer and enterprise use.

Its software-only solutions eliminate the need for expensive hardware or changes to user behavior.

RiskFort and WebFort's low TCO, easy deployment, and high scalability make them an ideal upsell to new and existing SiteMinder accounts to protect and verify user identities.

Q: What is the Arcot integration with SiteMinder?

A: Arcot integrated two of its software-only products with SiteMinder Web Access: RiskFort, a risk-based authentication product, and WebFort, a strong authentication product.

RiskFort – Risk-Based Authentication

Q: What is the value of risk-based authentication?

A: Risk-based authentication adds an invisible layer of fraud detection capability to your current authentication process. Because RiskFort automatically and invisibly collects and analyzes a range of data, it can detect when a fraudulent user is using legitimate credentials and impersonating a legitimate user. It can block fraud before any losses or data theft occurs.

Q: How does RiskFort work?

A: RiskFort collects data when a user tries to authenticate with a web portal or application. It analyzes data about the user and the authentication request (such as device ID, user behavior, location, context, organizational policies, etc.) and creates a Risk Score. This Risk Score measures the potential for fraud.

You can tailor the response to a specific Risk Score to match your policies and risk tolerance. Responses can include approving the authentication attempt, requesting additional information, limiting access to some applications/functions, referring the user to a customer service representative, or blocking it. All of this is transparent to legitimate users—only those users whose activity is unusual will experience any change to their login process.

Q: Why are usernames and passwords ineffective at stopping fraud?

A: Fraudsters have become very skilled at fooling users to visit fraudulent web sites and divulge their credentials. It is also easier, given easy online access to many public records, to make educated guesses at usernames and passwords based on personal information. The influence of organized crime on identity theft has created a strong market demand for credentials with which to impersonate legitimate users. Simple usernames and passwords are no longer sufficient to prevent unauthorized users from gaining access to your confidential or regulated data.



Arcot Customer FAQ

RiskFort & WebFort

Customer FAQ

WebFort – Strong Authentication

Q: How does Arcot address the challenge of Internet authentication?

A: Arcot provides software-only strong authentication that is the right balance of cost, convenience, and strength. Because Arcot's solutions are software-only, they scale up to millions of users, provide a convenient browser-based interface or VPN client plug-in for end users, and are easily deployed and managed. The sophisticated and proprietary technology approach Arcot uses delivers hardware-level security protection. In addition, Arcot designed its technology so that you can deploy it in a number of formats, including as a software-only container, or as a hardware container (such as USB tokens or crypto tokens). In addition to connecting with a wide variety of server applications, Arcot software can also provide a common interface for software smart cards, hardware smart cards, and USB tokens.

Q: What is the value of software-only strong authentication?

A: Strong authentication gives you a secure way to verify your users' identities, whether they are employees, partners, or customers. Strong authentication, also known as multi-factor authentication or two-factor authentication, uses two 'factors' to authenticate users – "something you know" and "something you have." It is more a secure method to verify users' identities than traditional username and password.

WebFort provides strong authentication completely in software, meaning that you do not have to incur the expense of purchasing, distributing, and managing alternative hardware-based technologies like one-time password (OTP) tokens, grid pads, or smart cards. In addition, the user experience is a familiar username/password, making Arcot strong authentication simple enough for a child to use.

Q: How does WebFort perform strong authentication?

A: WebFort requires your users to provide two 'factors' to verify their identity, completely in software. They provide "something they know", the password for the ArcotID, and "something they have", the ArcotID itself.

Q: What is the ArcotID?

A: The ArcotID is a secure software credential that combines protection for user identities like that of a hardware smart card with the low cost and benefits of a software solution. It is the software equivalent of a hardware smart card, providing a PIN-protected software container for the user's credentials: a standard X.509v3 digital certificate plus an encrypted private key. Arcot's patented design ensures that the ArcotID resists brute force and offline attacks, yet provides the strong authentication necessary to establish identity, create digital signatures, and decrypt documents.



Arcot Customer FAQ

RiskFort & WebFort

Customer FAQ

The ArcotID performs the authentication invisibly, so all your users see is a request for their username and password. It hides all the complex cryptography and PKI-based challenge/response that protects and verifies their identity from your users, making Arcot strong authentication simple enough for a child to use.

The ArcotID is a file that resides on your users' systems. You have complete flexibility to distribute the ArcotID to your users, whether enterprise or consumer. You can push out the ArcotID as part of a regular software update, deploy it on a USB drive or CD-ROM, or even deploy as invisible Flash client via your sign-on page. Your users can also download the ArcotID securely "On-Demand", giving them secure roaming access.

Q: What is unique about Arcot's authentication technology?

A: Arcot Systems is the only company that provides software-only authentication that combining the security of hardware solutions with the convenience of username-passwords.

Two key technologies form the basis of Arcot products: digital certificates—an industry standard—and Cryptographic Camouflage, a patented software technology developed by Arcot. The combination of these two technologies makes software-only strong authentication a reality.

Q: Where is the digital certificate and how does Arcot protect it?

A: The ArcotID stores the digital certificate in the ArcotID container. Arcot's Cryptographic Camouflage technology protects the private key from brute force attacks. The ArcotID enables credential access through a variety APIs, remaining transparent to the user. PKI-aware applications can use the ArcotID as a direct replacement for a hardware smart card using standard cryptographic interfaces.

Q: What is Cryptographic Camouflage?

A: Cryptographic Camouflage is Arcot's patented technique for protecting information in software. It differs from the standard encryption approach in that the attacker does not know when he has successfully uncovered the information. This approach provides security against offline attacks, allowing Arcot to offer strong digital signature and identity solutions in software.

When using a standard encryption approach, an intruder tries to reveal protected information with a variety of automated tools that conduct offline attacks. These techniques—including brute force, dictionary, and other types of attacks—try to guess the password until they find a plausible solution (i.e. a



Arcot Customer FAQ

RiskFort & WebFort

Customer FAQ

well-structured private key). With this approach, an attack will yield only one solution—the correct one that reveals the protected information.

Cryptographic Camouflage, on the other hand, yields what only appears like a plausible response. In other words, the attacker will not be able to determine which key is correct—it is hidden, or camouflaged, amongst a large number of plausible but incorrect solutions.

Keys produced as result of using an invalid password meet all the characteristics of a valid key, meaning an attacker can use them to encrypt or “sign” a challenge received from the WebFort authentication server. However, when the attacker uses the key to encrypt/“sign” the challenge and respond to the Arcot authentication server, WebFort will know that the key is not correct and increment the invalid password counter. Just as with a hardware-based solution like a smart card, the server can lock any access to the ArcotID software credential after a configurable number of invalid attempts (the default is three).

Q: What is a private key and why is it important to protect it?

A: A private key is one-half of the public/private key pair used in digital certificates. The private key is a software key used to sign challenges or documents. Similar to a physical signature, knowledge and use of the private key validates that the end user signed the challenge or document. Therefore, protecting the private key is critical to protecting the digital certificate and the user's identity online. If a third party gains access to a user's private key, the third party could easily masquerade as the user, commit fraud, and gain access to confidential information.

The private key is usually stored on the owner's system in a password-protected key container. Hackers and virus-software authors can use a variety of tools to collect and hack these key containers to collect private keys. Companies such as RSA, VeriSign, Sun Microsystems, and Baltimore Technologies, as well as technology analyst Gartner Group, have all cautioned users that protection of the private key is very important.

Q: How is the Arcot solution as secure as smart cards?

A: Smart cards and Arcot solutions both provide two-factor authentication. Both approaches require the user to have possession of something (the smart card or the ArcotID) and to know something (their password). Arcot's use of Cryptographic Camouflage protects the ArcotID from offline attack, making the card unusable without the password. In other words, the user always needs “something they have” plus “something they know” to ensure a successful login and using Arcot's strong authentication.



Arcot Customer FAQ

RiskFort & WebFort

Customer FAQ

Q: Does the ArcotID store a user's password, or transmit the private key to the WebFort authentication server?

A: No and No. The ArcotID never stores a user's password. It prompts a user for his password, but does not store the response. It uses this information to unlock the user's private key, which the ArcotID then uses to create a secure hash to transmit to the authentication server.

Q: Why is Arcot's software-only approach better than a One-Time Password (OTP) hardware tokens?

A: Arcot's approach is superior to OTP tokens for the following reasons:

1. Lower cost: OTP tokens are significantly more expensive to purchase, deploy, and manage. They have higher up-front (to acquire, distribute, and train users) and ongoing costs (to replace tokens due to loss/breakage/battery failure).
2. Easier to use: OTP tokens require a change in user behavior, as users must remember to bring the token with them any time they want network access. WebFort does not require any change in user behavior—it can install invisibly to the user and have the same appearance as the familiar username/password sign-on processes.
3. More secure: OTP tokens are vulnerable to sophisticated phishing threats called Man-in-the-Middle. These attacks can defeat OTP tokens and other one-time password technologies by capturing and relaying a user's credentials in real-time, bypassing the primary security feature of OTP tokens—that the password is 'live' for only 30-60 seconds. For more information, see the white paper "Protecting_Against_MITM.pdf".

About Arcot Systems

Arcot Systems provides risk-based authentication, strong authentication, digital signing, and cardholder authentication solutions. Arcot makes online transactions safe for millions of customers by blocking fraud and protecting access. Its 100% software solutions eliminate the need for expensive hardware and complex login processes. Arcot provides users with multi-factor, PKI-based authentication with the simplicity of a password.

Arcot Systems, Inc. | 455 West Maude Avenue | Sunnyvale, CA 94085 USA | www.arcot.com | +1 408 969-6100

Copyright © 2007 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.