PRODUCT SHEET:
CA Arcot WebFort

CA Arcot WebFort

CA Arcot WebFort® Versatile Authentication Server allows you to deploy a wide range of strong authentication methods in an efficient and centralized manner. It can increase security and improve your compliance profile without burdening users or your help desk. CA Arcot WebFort is integrated with CA SiteMinder® to provide a robust set of functionality which includes the management, execution and tracking of multiple authentication methods.

Overview

Usernames and passwords are the most common way for users to authenticate to web applications and portals. Unfortunately they are often a critical, weak link in a web security system and they can fail to satisfy many industry best practices or regulatory guidelines for protecting identities and data. All customers, employees, partners and contractors require secure, easy access to applications and networks. Organizations need to protect all of their users with a strong, cost-effective method of authentication, especially when it involves confidential, proprietary or regulated data.

Benefits

CA Arcot WebFort transparently protects and verifies your web users identities, without the need for expensive hardware or the need to change your users' familiar sign-on process. CA Arcot WebFort's cost-effective, user-convenient authentication enables you to protect all of your customers, partners and employees from identity theft and fraud. It is ideally suited for organizations that want to choose risk-appropriate authentication methods without having to install multiple vendor authentication solutions. You can also add strong authentication to unprotected users and help meet compliance regulations, without having to replace legacy hardware tokens.

Challenge: addressing a weak link

CA Arcot WebFort: Advanced Authentication

Usernames and passwords are easily cracked, stolen, or can be given away. When used as the only form of authentication, they can be a weak link in security which leads to identity theft and fraud. Traditionally, any enterprise wishing to upgrade users to stronger authentication faces deploying expensive hardware-based technologies: one-time password (OTP) tokens, smartcards, or USB drives. For enterprises with thousands of users, the cost to deploy hardware-based strong authentication can be prohibitive. Furthermore, these costly technologies also require changes to user behavior which result in significantly higher operational costs because of the increase in the number of calls to the help desk.

Strong authentication solutions are rapidly becoming a necessity for Internet-facing applications. However, wide-scale authentication deployments must do more than provide security; they must be able to scale with the global organizations that deploy them.

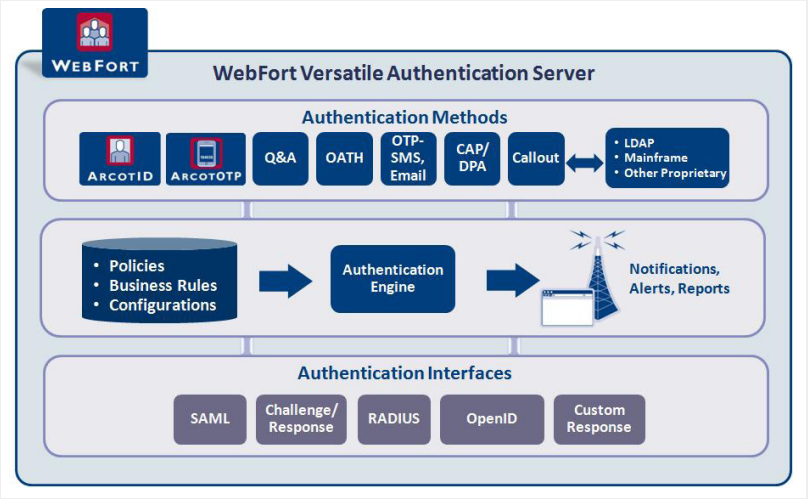
Solution: Versatile Authentication Server

Providing a choice of user-convenient authentication methods

CA Arcot WebFort is a versatile authentication server that allows organizations to protect all of their users with a choice of user-convenient, cost effective authentication methods. CA Arcot WebFort supports a range of authentication methods which include username/password, security Q&A, OTP via SMS, email or voice, OATH tokens, and the unique ArcotID and ArcotOTP.

Figure 1

CA Arcot WebFort Versatile Authentication Server



ArcotID: The ArcotID is a secure software credential that provides multifactor authentication without the cost or inconvenience of hardware. It gives you the freedom to strengthen any username/password authentication process by transparently upgrading users to software-only public key infrastructure (PKI)-based multifactor authentication. CA Arcot WebFort hides the sophisticated PKI-based challenge/response from your users, protecting their online identity while keeping the simplicity of a username/password. There is no need to change your users' familiar username/password-based sign-on experience or invest in expensive hardware to provide stronger authentication for customers, employees, or partners. The ArcotID's software-only form factor can simplify deployment and make it easy for individuals to use. In addition to computers, the ArcotID can be deployed on a mobile phone providing two-factor authentication from a user's mobile device.

ArcotOTP: The ArcotOTP is an all purpose secure software passcode generator that allows mobile phones, iPads and other PDAs to become a convenient authentication device. ArcotOTP supports standards including OATH (HOTP, TOTP) and EMV (CAP/DPA). The user's mobile phone runs the ArcotOTP application that generates the one-time-passcode (OTP). Users simply enter a pin, read the one-time-passcode and type the OTP into the application's authentication prompt. ArcotOTP allows users to easily generate an OTP to gain account access with a device that is already part of everyday life. ArcotOTP supports multiple accounts allowing users to have one app to run for access to many applications, VPNs and Web portals. Phone service is not required to use the ArcotOTP app. The ArcotOTP app is free and is available from the iPhone store, BlackBerry, Android Marketplace or from your application provider. You must be enrolled in the application provider's authentication program to use ArcotOTP.

Cryptographic Camouflage makes the difference: The ArcotID and ArcotOTP authentication methods use Arcot's patented Cryptographic Camouflage key concealment technology to protect credentials from brute force attack.

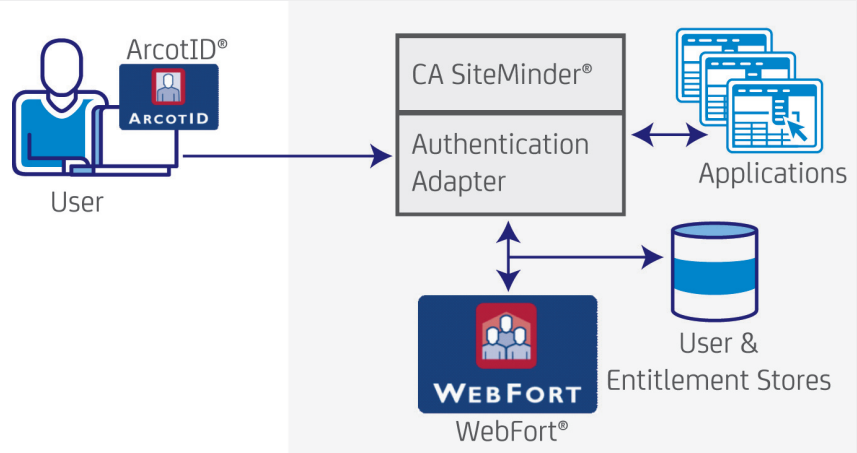
Integration with CA SiteMinder: Integration between CA Arcot WebFort and CA SiteMinder enables a robust Web access management solution that facilitates the management, execution and tracking of multiple authentication methods in an efficient manner. CA Arcot WebFort capabilities or services are visible within the CA SiteMinder policy management interface and can be applied to a select set of applications and users or across the entire enterprise. These powerful advanced authentication processes can be configured within the CA SiteMinder environment for the initial user authentication, step-up authentication for sensitive applications or specific SSO zones.

Anytime, anywhere access: CA Arcot WebFort's roaming capability enables your users to maintain their anytime, anywhere access to your critical applications, information, and services. When users are away from the PC they typically use, they can quickly verify their identity through a variety of secondary authentication methods including knowledge-based Q&A or OTP to SMS or email, and gain roaming access.

Figure 2

CA Arcot WebFort as part of a secure CA SiteMinder environment

CA Arcot WebFort provides a multi-factor authentication solution that integrates seamlessly with your CA SiteMinder environment.



Business benefits

Deploy multi-factor authentication invisibly: Your Web users never have to know that you upgraded them to multi-factor authentication, unless you want them to. They can keep the same username/password sign-on experience with which they have become so accustomed. CA Arcot WebFort invisibly protects and verifies their identity without burdensome additional login steps.

Lower cost of ownership: The CA Arcot WebFort versatile authentication server allows you to authenticate users with a wide range of authentication methods. It can help you manage your authentication environment more efficiently by creating a central point for authentication policy creation and enforcement. If you use the ArcotID software-only approach, there is no hardware to lose, fail, or break. It provides a low cost, easy to distribute second factor authentication method that hardware-based alternatives cannot match. The simplicity and transparency of this approach helps reduce both management and support costs.

Reduce risk: Multi-factor authentication helps reduce the risk of identity theft and online fraud by requiring the second factor to access Web resources. CA Arcot WebFort centralizes the management and execution of strong authentication. It authenticates users via a wide range of methods, giving you the flexibility to choose the authentication methods that best suit your user

groups. It also helps you manage competing compliance demands by creating a central point for authentication enforcement. When the ArcotID is used as the second factor it helps protect the digital identities of your users behind proven, patented cryptographic technology.

Block Man-in-the-Middle (MITM)/Man-in-the-Browser attacks (MITB): CA Arcot WebFort when used with ArcotID, helps prevent MITM attacks. The ArcotID authenticates only with the domain that issued it, helping protect your users from Phishers and Pharmers where OTP tokens and Grid Pads cannot. Patent-pending Virtual Private Sessions help prevent MITB attacks which involve alteration or hijacking of data in sessions.

Meet regulatory requirements: CA Arcot WebFort is used to help meet a number of government regulations and industry standards for stronger Web authentication, including FFIEC, SOX, HIPAA, SAFE, and IdenTrust.

Achieve high-performance: CA Arcot WebFort is the core of Arcot's authentication architecture. To meet the rigorous security, availability, and data integrity demands of the financial services industry, Arcot designed WebFort from the start to provide the strongest security and performance possible. To provide authentication services to millions of users, Arcot designed CA Arcot WebFort with virtually unlimited horizontal scalability, with a goal of unparalleled ease-of-use and extremely low latency.

Enjoy virtually unlimited scalability: CA Arcot WebFort provides excellent vertical scalability through increasing memory/disk/processors. It achieves full-featured horizontal scalability with additional local or remote servers. Horizontal scalability provides performance gains as well as high-availability features for critical deployments. You can protect millions of Web users without degrading application or network performance. When combined with CA SiteMinder, a leader in Web access management performance and scalability, the solution provides the flexibility and reliability necessary in an enterprise environment.

Future-ready authentication: CA Arcot WebFort provides the foundation for you to upgrade to other valuable business services like secure delivery of eBills and eDocuments or digital signing of forms and documents, when you are ready.

On-premise and cloud deployment options: CA Arcot WebFort is available as a cloud service or it can be installed on-premise. The same functionality is available no matter which deployment option you choose. Today, our cloud computing services serve over 70 million users worldwide and are hosted in multiple SAS 70 Type II audited, PCI DSS-compliant data centers. Our cloud services are highly scalable, configurable, and multi-tenant efficient. By utilizing CA Arcot WebFort strong authentication in the cloud you can help eliminate the headaches associated with installing hardware and software on-site by reducing costs and management overhead.

The CA Technologies and Arcot advantage

CA Arcot WebFort delivers additional identity protection for your Web applications and portals. Whether you want the automated software token method (ArcotID), or the one-time password method (Arcot OTP), or both, Arcot's versatile authentication adds additional protection to your critical data and applications. It can help to quickly and easily add multi-factor authentication to your SiteMinder protected Web applications and portals, without changing your users' familiar username/password sign-on process. CA Arcot WebFort can eliminate the need for expensive tokens or cards, giving you increased security and high performance and scalability with a low cost of ownership. Arcot's software-only approach gives you the right balance of cost, convenience, and strength for enhancing the protection of your Web resources and the identities of your Web users.

CS0069_1110.