

# Technology Audit

## Security

### Arcot Systems Inc.

Written by: Andy Kellett

### Arcot WebFort/ArcotID – version v1

Date: November 2006

#### Abstract

Arcot Systems Inc. is a recognised provider of strong authentication and digital signing products. The company's WebFort (authentication server) and ArcotID (authentication token) solution provides a software-based approach to the delivery of secure user authentication services. The product is in essence a two-factor strong authentication credential for the management of digital identities that is completely software driven, and whilst providing strong certificate-based two-factor authentication the Arcot solution looks exactly like a user-name and password product. WebFort, which is written in C++ and Java, provides Arcot's authentication server facilities, and works alongside the ArcotID software smartcard authentication token to deliver a flexible range of authentication services that can be configured to operate within multiple Identity Management (IdM) operations, such as Public Key Infrastructure (PKI), One-Time-Password (OTP), RADIUS, and SAML environments. In operational use, the Arcot solution can provide the interface to a variety of applications including Web portals, e-mail systems, Virtual Private Networks (VPNs), and can be positioned as the front-end component to an organisation's Access Management and Single Sign-on (SSO) systems. The business community, especially organisations that work in the financial services and retail sectors and provide on-line services, continually struggle to find IdM and user authentication solutions that are capable of dealing adequately with identity theft. This is the role that Arcot has set for itself and its product success should be measured on its ability to fully address the protection needs of on-line traders and service providers.

#### KEY FINDINGS

Key: ✓ Product Strength ✗ Product Weakness i Point of Information

✓	Multi-functional solution that can be used to deliver strong authentication, digital signing, and encryption services.	✓	Provides two-factor authentication that operates without the need for a hardware interface.
✓	Ease-of-use and ease-of-distribution are seen as key assets of this software-driven IdM solution.	✓	Operates alongside and supports the use of PKI, OTP, and secure VPN solutions, and supports a wide range of third-party CAs.
i	Server platforms supported include: Sun Solaris and Microsoft Windows.	i	Databases supported include: Oracle and Microsoft SQL Server.
✗	It would benefit from extending the range of platforms supported to include AIX and Linux.		

#### LOOK AHEAD

Going forward Arcot is looking to position its authentication solution as a key component of IdM. To achieve this objective the company is focusing on adding its strong authentication solution to existing IdM platforms, SSO products, and VPN vendors. Arcot will also be extending its range of supported platforms. For example, the company will make the ArcotID client more ubiquitous through partnerships with organisations such as Adobe, where Arcot is currently embedded in Acrobat and Reader 8.

## ► FUNCTIONALITY

When, as corporate users or private individuals, we logon to computer systems, we expect that the work that we do, the communications that we respond to or bring about, and the transactions that we instigate, will be adequately protected; and that such actions should not put at risk the integrity of our businesses or our own personal information. Unfortunately, on many occasions, this is not the case. Either the systems that we interact with are inadequately set up and protected, and their deficiencies can be exposed by a range of real-time or latent attack models, or the security facilities that are provided to identify us as authorised systems users fall short of what is required to ensure that a third party cannot steal that identity and use it for their own purposes. Amongst other threats, Phishing, Pharming, Man-in-the-Middle (MIM), Trojan, and Key-logger activity all represent forms of corporate and personal attack approaches that threaten the way that we freely access computer systems and the information that they hold. Across the security industry a wide range of protection technologies have been developed to overcome such malicious activity, some are very good at what they do, others less so, but all provide at least some levels of benefit.

Arcot is positioning its ArcotID and WebFort product suite as key components in the IdM and strong authentication sector of the security industry. This is a highly competitive area of the protection marketplace and one that has achieved a very high profile over the last three years. However, whilst other players in this space mainly focus on the use of hardware and smartcard-based authentication solutions to deliver their identity and authentication solutions, Arcot differentiates itself from such mainstream approaches by providing a software-based alternative that is capable of dealing with all current identity-driven attack models.

### Product Analysis

There are three key components that make up the Arcot solution – ArcotID software token, ArcotID Client software, and the WebFort server. They provide single source user identity services for authentication, digital signing, and encryption and decryption.

**ArcotID** – provides a unique and patented file-based software approach to the protection of the private key of a Public Key Infrastructure (PKI) key pair. Its software approach, known as ‘Cryptographic Camouflage’ is a technique that takes the password that a user provides and encrypts the PKI private key in a way that is completely resistant to brute force attacks, enabling the private key to be securely stored within a small file. As ArcotID is a software solution, and because of the files secure nature, flexibility is afforded to the way that its services can be utilised. As determined by the end-user organisation’s requirements and risk policy the ArcotID file can be held on a user’s PC or carried separately using portable media such as a CD or USB stick. Alternatively, and if appropriate, it can also be downloaded from a secure Web site.

The **ArcotID client** – is available on the user’s desktop and provides the interface for the end-users preferred applications, for example, as the login page to a Web portal. The ArcotID client is available in various forms including an unsigned Java applet or Flash or Javascript that can be included with a Web page, installable client software, a signed Java applet or Active-X control. In essence, ArcotID is a strong two-factor authentication solution where the identity file and the user password are stored separately (one is the file – something the user has and the second is the password – something the user knows, they both have to come together and operate for the authentication to succeed), and neither can be derived by knowing or intercepting the other. Functionally, ArcotID provides all the serviceability and security components of a PKI-based smartcard (including CSP and PKCS#11 interfaces), but because it is a software alternative it also adds ease-of-distribution, portability, and user simplicity into the mix.

**Arcot WebFort** – is the solution’s authentication server. It works alongside ArcotID to provide a complete user authentication solution, and in support of each end-user organisations own operational requirements, the WebFort server can be configured to operate in different modes. For example, it can be configured to support PKI and OTP requirements and can also support the requirements of RADIUS and SAML environments. Operationally, it provides easily constructed, ready-made interfaces to a wide range of identity-driven applications, including Web portals, e-mail systems, Virtual Private Networks (VPNs), and can be utilised to front-end the Access Management and SSO components of an I&AM solution.

It also includes the RiskFort authentication risk management product. RiskFort evaluates each on-line access event for its potential to be fraudulent. The risk analysis engine calculates a risk score of each authentication attempt based on a number of variables, such as device identity, IP address, location, and the context of the transaction (e.g., amount or type of transaction). The risk score is a measurement of the fraud potential of an authentication attempt, from 0 to 100 (the higher the score, the higher the potential for fraud). In addition, organisations can apply additional rules, such as user profiles or business policies, to the transaction analysis before determining appropriate actions. Such actions may include: allowing or denying access, requesting additional Out Of Band (OOB) information, or sending messages/alerts for further review.

Where in Butler Group’s opinion, the Arcot authentication solution differentiates itself from other mainstream authentication tools is in its ability to support digital signing and in the way that it ensures that a users digital identity cannot be compromised by any current type of electronic identity theft approach. This includes: Phishing; Pharming; MIM; Trojans; Key Loggers; Replay Attacks; Brute Force; Non-Repudiation (or fraudulent administrator); Plaintext; Challenge/Response Intercepts; and Private Key Exposure. All of which is achievable because Arcot’s software-based challenge/response approach has been designed to ensure that the private key being used to authenticate an ArcotID request remains secure and is only ever available when the authentication response is signed. At a more detailed level, and as shown in the Figure 1 user authentication diagram below, when an access request is sent using ArcotID the WebFort authentication server first sends out a challenge in the form of a random character string. When the user responds by providing their correct access code, PIN, or private key, ArcotID signs the response and sends it back to the WebFort authentication server. Only the response is sent back to the authentication server for verification. The access code, PIN, or private key is never stored or transmitted, and therefore, using existing real-time attack techniques such as MIM, it cannot be captured and successfully reused.

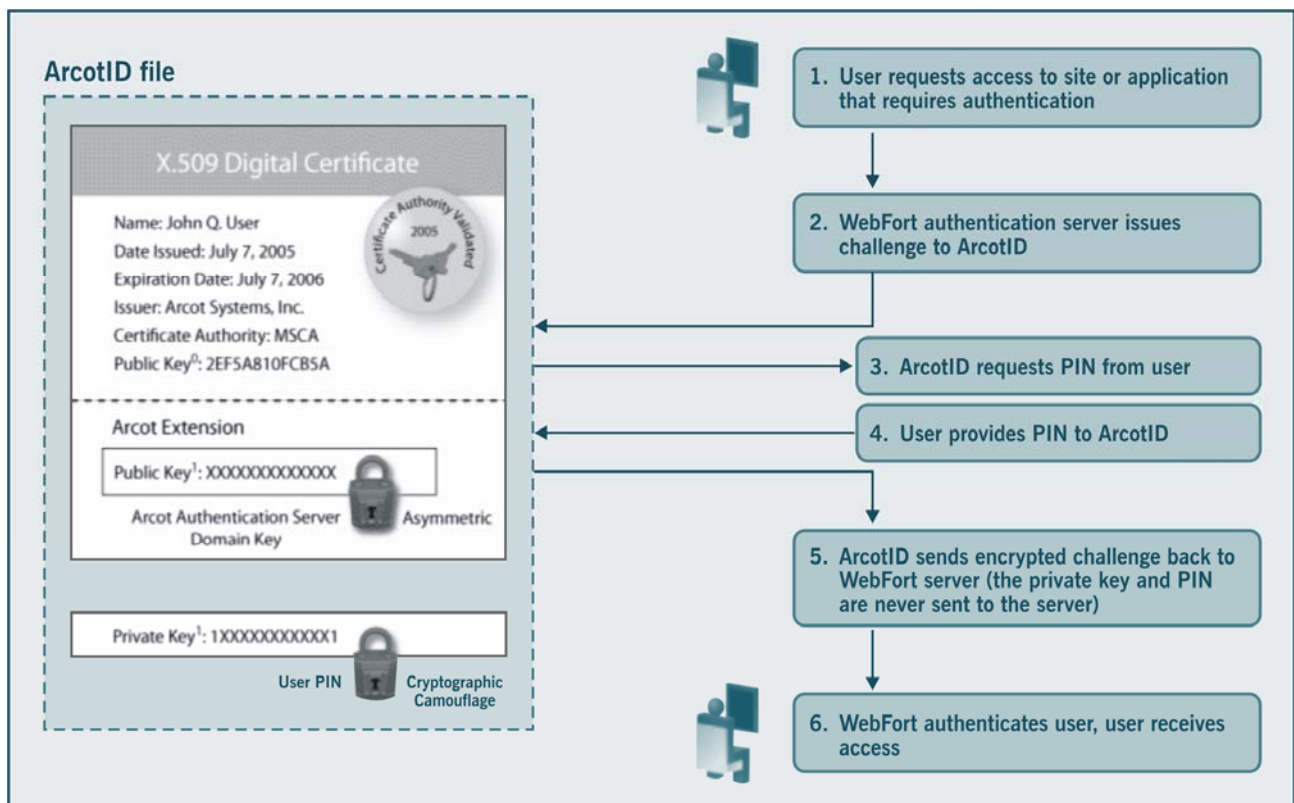


Figure1: Using ArcotID and the WebFort Server for User Authentication

For those organisations that require other additional levels of PIN and password access control protection, Arcot also provides an optional keypad scrambling facility that can be used to further protect against sniffer activity and keystroke loggers.

---

## Product Operation

---

In operational use, the software components of ArcotID provides its protection services in a very similar way to that of a smartcard, hardware token, or other secure authentication tool. In fact, it can be positioned as a software smartcard that delivers a secure private key container in the form of a software file, but then incorporates the use of a camouflaged software layer that is capable of fully repelling 'brute force' or any other form of attack that derives its success from identifying and exposing private keys. Using the company's patented 'Cryptographic Camouflage' technology the private key is encrypted based on the users PIN, using standard encryption algorithms alongside the company's secure protection processes. As a result, and this is where the camouflage elements of the solution come into play, each time a PIN code is entered; even an incorrect PIN code, the system will produce a properly formed private key that follows system specified and formatted characteristics. For example, based on a six-digit numerical pin, one million keys would be produced, and if alphanumeric characters are used then the possible combinations would exceed two billion. As the length of the PIN increases, the number of permutations increases exponentially. Authentication is not successful unless the appropriate challenge/response dialog occurs with the Arcot Authentication Server. The usage of the correct PIN, and thereby the authentication of the genuine user, can only be determined by performing this authentication step.

Each of these generated keys can be used to encrypt and sign an Arcot generated challenge from the WebFort server. However, none of these keys, other than the valid string where one exists, can be accepted to provide valid access authentication to the system, and for the attacker each generated key needs to be tested by signing it individually in order to determine its pass or fail status. Where access is denied due to an invalid access attempt the invalid PIN counter is incremented and determined by corporate policy – access can be locked if an unacceptably large number of invalid access attempts are made.

The ArcotID provides two-factor authentication by linking the information that the user knows – their PIN, access code – to their ability to successfully access the ArcotID secure digital identity container, and complete the authentication transaction by sending back the generated response to the WebFort Authentication Server. In addition, because of the open nature of the Arcot solution, it is able to support a good range of authentication approaches including: PKI-based digital certificates that can be accessed natively through standard interfaces such as Microsoft CSP and PKCS#11; ArcotID, that looks like a username/password and is the default standard using native APIs and plug-ins to generate appropriate challenge responses; and OTPs that can be generated using Arcot authentication facilities. WebFort also supports plain simple username/passwords – and provides a single authentication server when customers want a mixed mode deployment.

To provide a detailed example of an Arcot authentication sequence, there are six stages to using Arcot natively via an API and a similar sequence of events would also be undertaken when requesting Arcot controlled access via other associated channels such as VPN or OTP secured access:

1. User requests access to their authorised Web application or systems resource.
2. The system front-end directs the request to the Arcot WebFort authentication server.
3. The WebFort authentication server sends an access challenge back via the systems front-end.
4. The user enters their access credentials (PIN, access code, or certificate details) in order to de-camouflage the private key. The challenge is then signed and returned to the authentication server.
5. The authentication server decodes the signed challenge and sends a success or fail message back to the systems front-end.
6. If successful, the front-end system sets up a secure user session to the requested application or systems resource.

---

## Product Emphasis

---

The key functionality of the ArcotID and WebFort product suite that in Butler Group's opinion, makes the offering particularly attractive as a strong authentication solution, revolves around its ability to deal with all forms of identity-focused attack models, its software only approach, and its digital signing and decryption capabilities. In addition, the open nature of the solution enables it to efficiently deal with all allowable access requests irrespective of machine source, location, or access channel, making it appropriate to meeting the needs of a wide range of Business-to-Business (B2B) and Business-to-Customer (B2C) environments. In addition, the look and feel of 'user name and password' makes the solution easy-to-use for employees, partners, and consumers.

## ► DEPLOYMENT

Under normal circumstances, a standard installation of the ArcotID and WebFort product set requires virtually no elements of technical expertise other than the ability to install Operating System (OS) components, the supporting database, and where required, an appropriate HSM and CA. However, additionally, it is often the case that end-user organisations will choose to integrate the WebFort component of Arcot's offering within their existing I&AM infrastructure. To date, the solution has been successfully deployed alongside I&AM solutions such as IBM Tivoli, CA/Netegrity, and Oracle, with additional integration work being undertaken by the company's professional services team or by a third-party Systems Integrator (SI).

Currently the WebFort Server runs on Sun Solaris and Microsoft Windows servers, and further platform options including IBM AIX and Linux are planned. The server interfaces with Oracle and Microsoft SQL Server databases, with IBM DB2 on the planned roadmap. ArcotID service delivery has the flexibility to utilise the company's own inbuilt Open SSL CA, or can operate using certificates from other certificate authorities, and under such circumstances interfaces already exist to work with Verisign, Entrust, and CyberTrust, and optionally, to achieve added security, master domain keys can be stored on HSM devices from nCipher and Safenet Luna. A large number of VPN and SSL VPN vendors are supported, including Check Point, Cisco, F5, Juniper, and Aventail.

The average implementation timescales for deploying the Arcot solution is measured in weeks rather than months. However, for more complex implementations that involve significant integration work and professional services assistance, these projects can take from three to four months to complete – an example of this is one particular deployment to 20 million users which, from start to finish, took only a few months to complete. Once deployed, the WebFort server requires only a limited amount of management resources, with administrators being tasked with monitoring server logs for specific organisational actions, in this respect they could also be tasked with providing help-desk support for users who need assistance with the self-service elements of issuing new ArcotIDs or those that need help to recover lost access codes. Product training can be provided through a combination of Web-based and on-site sessions. In addition, the delivered product set includes detailed usage documentation that enables administrators to walk-through various case scenarios and provides guidance on systems and product requirements. Also, Arcot provides a Web portal for customers to log issues, and its support team is able to provide 24x7 monitoring and support services.

## ► PRODUCT STRATEGY

Arcot is currently pursuing a vertical market strategy for the deployment of its product suite. Using this approach, it has to date, been particularly successful in areas such as Financial Services including brokerages and the banking and payments sectors, B2B segments, Government, and Pharmaceuticals. Going forward, the areas that have been identified as providing significant growth opportunities include: the Retail sector, Corporate Banking, On-line Consumers, and Enterprise Security – particularly in B2B environments.

ArcotID and WebFort products are sold primarily through direct sales channels. However, the company's ongoing strategy is to make initial market wins through the direct sales channel, and then make use of such relationships to develop partnerships. In this respect, Arcot has a history of working with partners with its other products. For example the company's TransFort solution for payment authentication has been sold extensively through partners such as: First Data; Certegy; PEMCO; Metavante; FIServ; and Shazam, and this sales relationship has been extended to include SIs such as: IBM; HP; and Unisys. Going forward, Arcot is looking to establish its authentication products as a key part of the IdM stack and is working with other players in that space to achieve this objective.

The company states that Return On Investment (ROI) can be calculated on a number of different levels for the key components of its ArcotID and WebFort solution, including: a risk-based model; a compliance model; and a consumer confidence model. A risk-based model takes into account the values that can be placed on preventing fraud from occurring. A compliance model measures the lower costs of deploying Arcot's software-based authentication solution (as opposed to hardware-driven alternatives in order to achieve regulatory requirements). A consumer confidence model calculates the number of additional customers that can be persuaded to move to using low-cost Internet channels by improving their security facilities. Finally, and specifically for the financial services sector, reducing the need for paper-based customer statements through the promotion of secure, electronically delivered e-statements significantly reduces recurring operational costs.

For pricing, customers licence the Arcot product on a per-user per-year basis for a term of three or more years. The price includes all necessary WebFort server and ArcotID client components, with a scale that reduces by volume. The average project value for an Arcot deployment can vary significantly as the user base scales from organisations with a few hundred users to 20 million at the top end of the range. Smaller projects begin at around US\$20,000 for a three-year contract and up to tens to hundreds of thousands of dollars for larger deployments. Standard annual maintenance charges for the server are set at 18% of the license fee.

### ► COMPANY PROFILE

Arcot is a privately-owned company and has its corporate headquarters in Sunnyvale, California, in the US. It has major development, support, and services offices in Bangalore, India, and has multiple sales offices across the US, in the UK (London), and in Germany. Ram Varadarajan was a company founder in 1997 and remains as company President and CEO. Funding for the company has come from private venture capitalist and corporate sources including: Onset Ventures; Accell Partners; Goldman Sachs; and SEB; and Arcot has also received strategic investments from Adobe; Visa; Oracle; and Novell.

Arcot currently employs over 100 staff, with around 35 based in the US, 60 in India, and the rest in Europe. As a privately-held company Arcot does not publicly release its financial performance figures. However, it was prepared to confirm that its revenues are growing significantly on a year-on-year basis. Also, as the company trades in the IT security sector, it is difficult for it to name specific customers, although it was able to verify that the ArcotID and WebFort technology is in use by around 30 customers, and that because of the embedded nature of the company's other financial products its solutions were being used by over 50 million users during 2006. Arcot is also a leading supplier of secure on-line payment solutions, including 3-D Secure (Verified by Visa and MasterCard SecureCode). These technologies are deployed to over 11,000 banks and 25,000 merchants.

### ► SUMMARY

The ArcotID and WebFort products are now positioned as providing a key software-based approach to IdM and strong user authentication. As stated at the beginning of this Technology Audit, this is a highly-competitive area of the protection marketplace, but also one that must have the capacity to provide digital identity controls that are capable of supporting the needs of an extremely wide ranging user community. Butler Group believes that Arcot is able to achieve this, and at the same time differentiate itself from other mainstream authentication suppliers through its ability to provide a secure software-based approach to user authentication that is capable of dealing with all current identity-driven attack models, whilst also making use of the solutions challenge/response approach to ensure that private authentication keys remain highly secure.

## Contact Details

### Arcot Corporate Headquarters

Arcot Systems  
455 West Maude Avenue  
Sunnyvale  
CA 94085  
USA

Tel: +1 408-969-6100  
Fax: +1 408-969-6290

www.arcot.com

### Arcot International UK Office

Trinity Court-A  
Wokingham Road  
Bracknell  
Berkshire, RG42 1PL  
UK

Tel: +44 (0)1344 668 280  
Fax: +44 (0)1344 668 180

www.arcot.com



### Headquarters:

Europa House,  
184 Ferensway,  
Hull, East Yorkshire,  
HU1 3UT, UK

Tel: +44 (0)1482 586149  
Fax: +44 (0)1482 323577

### Australian Sales Office:

Butler Direct Pty Ltd.,  
Level 46, Citigroup Building,  
2 Park Street, Sydney,  
NSW, 2000, Australia

Tel: + 61 (02) 8705 6960  
Fax: + 61 (02) 8705 6961

### End-user Sales Office (USA): Important Notice

Butler Group,  
245 Fifth Avenue, 4th Floor,  
New York, NY 10016,  
USA

Tel: +1 212 652 5302  
Fax: +1 212 202 4684

This report contains data and information up-to-date and correct to the best of our knowledge at the time of preparation. The data and information comes from a variety of sources outside our direct control, therefore Butler Direct Limited cannot give any guarantees relating to the content of this report. Ultimate responsibility for all interpretations of, and use of, data, information and commentary in this report remains with you. Butler Direct Limited will not be liable for any interpretations or decisions made by you.

For more information on Butler Group's Subscription Services please contact one of the local offices above.