

**Filing Information**

June 2002  
IDC #27518  
Volume: 1  
Tab: Vendors

# Internet Security Software

## Bulletin

### **Arcot Systems Vendor Profile: Securing Digital Identities**

*Analysts: Charles Kolodgy and Chris Christiansen*

#### **IDC Opinion**

*What technology has Arcot Systems pioneered to make the Internet a better place to do business?*

Arcot Systems has patented a technology that can securely protect a digital identity and the contents of a private key using software only. With this and other innovations, the company has created a multidimensional platform for strong authentication, digital signing, and the protection of electronic identity that requires no hardware smart card or token. This software-only approach allows for greater portability and lower cost over hardware authentication solutions, and improved security over other software options. Arcot solutions bring new security options to existing applications, as well as enable new applications in the areas of online payment systems, business portals, Web services, and virtual private networks (VPNs).

## In This Vendor Profile

This bulletin provides background information on Arcot Systems. The company's solution platform for protecting digital identities and securing transactions is gaining acceptance as a means of providing strong authentication for ebusiness and IT applications. Portions of the Arcot architecture are in use today, providing the authentication platform for secure online payments for Visa International's "Verified by Visa" program. Arcot's products facilitate the use of public key technology for corporate extranets, business portals, and Internet transactions by providing hackerproof protection for an individual's private key. The company has been making inroads in a number of Internet security markets, including Web single-sign-on (SSO) and transactional security.

## Situation Overview

### *The Internet for eCommerce*

The Internet has grown from being an avenue for information exchange to being a medium for business interaction. IDC estimates that in 2001, ecommerce generated \$615 billion in transactions. By 2005, the value of online transactions should exceed \$4.5 trillion. As the Internet has become an important business channel, it has become imperative that users be authenticated and identified as a valid party, and have critical information protected. Although the need for authentication is paramount to business integrity, authentication has been neither easy nor affordable to implement.

Historically it has been very difficult to protect digital identities and critical personal information. All metrics report that incidents of hacking and Internet vulnerabilities are increasing at an alarming rate. Specific incidents associated with digital identities and personal data like credit cards include:

- Customer credit card information was obtained by hackers from the Playboy.com site in November 2001.
- Information for up to 98,000 customers could have been exposed from the Bibliofind.com in the spring of 2001.
- 55,000 credit card numbers were exposed to a hacker from the Creditcard.com website in December 2000.
- 350,000 credit card numbers were stolen from CDUniverse's site and posted on the Web in December 1999.

---

**Quoting IDC Information and Data:** *Internal Documents and Presentations*—Quoting individual sentences and paragraphs for use in your company's internal communications does not require permission from IDC. The use of large portions or the reproduction of any IDC document in its entirety does require prior written approval and may involve some financial consideration. *External Publication*—Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2002 IDC. **Reproduction is forbidden unless authorized.**

For additional copies please contact Cheryl Toffel, 508-935-4389.

*Check us out on the World Wide Web!*

<http://www.idc.com>  
Printed on recycled materials. ♻️

- The “John the Ripper” case: 186,000 worldwide passwords cracked in August 1998.

With all the threats and vulnerabilities to critical ecommerce data and digital identities, there is a special need to protect this information. There are many products and technologies included in IDC’s authentication, authorization, and administration (3A) security software market that try to solve the identity problem. The traditional authentication mechanism is a combination of username and password or personal identification number (PIN). These are sufficient to meet the needs of many closed environments, but for higher-value Internet services and transactions, they are not sufficient.

### ***The High Cost of Transacting Business***

There are costs associated with Internet transactions and ensuring their integrity. A system that can easily and cost-effectively authenticate and validate the identity of the parties involved in a transaction must be developed. The system must be able to provide nonrepudiation (i.e., prove the existence or execution of a transaction).

For stronger authentication needs, enterprises have turned to Public Key technologies (digital certificates) and to hardware solutions such as tokens that replace or issue one-time passwords, and smart cards that store authentication information (including certificates). However, these solutions are costly, hard to use, and difficult to get into the hands of customers — especially with the proliferation of client devices.

Transactional security is a balancing act between the friction that security creates in the business process and the level of risk a lack of security presents. Arcot Systems has developed a technological solution that leverages public key certificates, but does so in a way that is simple to use and deploy while reducing security costs and maintaining a high level of security. Arcot has created an end-to-end authentication platform that delivers the security, versatility, and usability required for a range of ebusiness and IT applications.

### ***Cryptographic Camouflage in a Nutshell***

Arcot has created a patented secure software container (the ArcotID Software Smart Card, or “ArcotID”) for private keys and digital certificates. This container offers tamper resistance through a process called “Cryptographic Camouflage.”

The ArcotID tamperproof container can be securely stored with the user (client) and is automatically invoked when user authentication or signature is required. The user activates the ArcotID with a simple PIN entry — through a user interface that can be made to look just like a username/password “login” screen. The authentication process requires no hardware device or reader and is seamless for the user. In this way, the authentication is easy, useable, and requires no end-user training.

Private keys stored on a computer are susceptible to attack. Normally, when stored in software, the key is encrypted with a simple PIN. This encrypted key can be copied and attacked offline by testing every PIN (a brute force attack). In the case of a six-digit PIN, that would mean testing 1,000,000 combinations. This seems like a lot, but for a computer, it would be trivial to break. In addition to testing the PIN, the structure of the resulting number is tested to determine if it meets the requirements of a key. Once the key is extracted, anyone can use it to impersonate the valid user.

*With Cryptographic Camouflage, Arcot Systems has developed a simple mechanism to protect the private key stored in software. Cryptographic Camouflage is an encryption algorithm that will always return what appears to be a valid private key, even when the wrong PIN has been entered.*

To better protect private keys, they can be stored on a smart card or USB token, where brute force attacks are not possible. However, with Cryptographic Camouflage, Arcot Systems has developed a simple-to-employ mechanism to protect the private key stored in software only. Cryptographic Camouflage is an encryption algorithm that will always return what appears to be a valid private key during a hacker attack, even when the wrong PIN has been entered. For every PIN entry attempt, the system returns a number adhering to the structure of a standard private key. For the six-digit PIN mentioned above, there would be 1,000,000 plausible numbers. The hacker would take the first seemingly correct response and attempt their fraud with that. After a few attempts the hacker would be locked out of the system.

With Cryptographic Camouflage, the information on the ArcotID is protected from key extraction and brute force attack, as is the information that is stored on a hardware smart card. The odds that a hacker would pick out the correct PIN are very small, not much less than the hacker's being able to randomly guess a smart card holder's PIN. The PIN is known only to the user and never stored on a server or locally. Keeping the user in control of their private key and personal PIN, the ArcotID offers users confidence that they control their identity on the Internet. Because the ArcotID protects the user's credential entirely in software, the user is able to freely roam and benefits from greater portability, convenience, and usability.

### ***Multikey Protection and Use***

Cryptographic Camouflage can be leveraged to provide the same level of protection to multiple private keys using Arcot's Key Authority functionality. Any number of "application" private keys and their associated certificates can be loaded on to the ArcotID, enabling the credential to act like a multiapplication smart card, where different certificates can be used to authenticate or sign for different purposes. The ArcotID can be used to protect certificates and private keys from leading trusted authorities, such as VeriSign, Entrust, Identrus, and Baltimore.

To access the "application" keys stored on the ArcotID, users first authenticate with the ArcotID to a Key Authority server. Upon successful authentication, users are given a partial secret to be used in conjunction with the other part stored locally to decrypt and access their application keys. These keys can be used to easily integrate with other systems or applications using standard interfaces. This process is transparent to end users, who select their

ArcotID and enter the associated PIN. The authentication, the delivery of the partial secret, and the use of the application private key are all performed behind the scenes. Applications that directly access these digital credentials do so using industry-standard cryptographic interfaces, such as PKCS#11 and Microsoft Crypto API.

### ***Arcot Applications***

Arcot has built an architecture for securing digital identities and transactions that is versatile, extensible, and easy to deploy. WebFort and TransFort are standalone solution components of this architecture that can be deployed independently or together, based on the needs of the application at hand. WebFort enables the secure roaming and multikey protection capability of the ArcotID (see above). TransFort is a server-side payment or transaction authentication platform that verifies the buyer to the seller and to the payment system at the time of purchase.

TransFort has gained acceptance with banks, processors, merchants, and merchant aggregators because it:

- Provides support for both Visa's "Verified by Visa" and MasterCard's protocol
- Supports both wired and wireless clients
- Provides functionality necessary for both merchants and card issuers
- Provides other support for nonrepudiation, enrollment, and authentication

### ***Secure Online Payments***

Arcot has been working with Visa International on its Verified by Visa program for over two years to develop a low-friction, easy-to-deploy means of authenticating a cardholder during an online transaction. Offering three levels of authentication security, including a personal password, an optional ArcotID, or an optional physical smart card, Arcot's TransFort product is being implemented by leading issuers, card processors, and merchants for the Verified by Visa program, and has been adopted by First Data Resources, the industry's largest card processor. Arcot's TransFort solution has been extended to support other payment systems, most notably MasterCard.

### ***Business Portals***

ArcotID Software Smart Card can be deployed alongside authorization solutions to meet the need for scalable, strong authentication in Web SSO environments. Enterprises are struggling with the challenge of managing burgeoning, distributed end-user communities desiring access to more Web-based applications, while still wanting to have protected privileges, confidential information, and ebusiness transactions.

Arcot's WebFort product offers authentication and signing features comparable to those of a physical smart card at a lower cost, with easy deployment and a simple customer interface. WebFort is being used by Bechtel Corp. to protect access to a business development portal, and by Swedbank to authenticate access to its online banking and brokerage services.

### *Web Services*

Web services needing strong authentication must be well protected without compromising the convenience and accessibility of the Web-based interface. WebFort is currently employed by Inovant, the information services group within Visa, as a replacement for hardware-based authentication to secure Web access to Visa's email service. WebFort combines the portability and usability required for strong authentication to Web services, particularly for mobile, roaming groups of end users.

### *VPN Authentication*

VPNs protect data in transit, but the vast majority of VPNs employ only a user name and password for login authentication. Arcot for VPN is enjoying increasing acceptance as an affordable and effective means of strongly authenticating the VPN user. Arcot for VPN can deploy alongside hardware token populations, as users are migrated to the ArcotID for a cost-effective, user-friendly solution. Arcot for VPN works with Checkpoint (as an OPSEC-certified product) as well as Cisco and Nortel VPNs. Customers for Arcot for VPN include State of Ohio PERS and Edix, a healthcare provider using Arcot for VPN to protect sensitive medical images and records.

### **Future Outlook**

Arcot Systems has products that can meet a number of authentication requirements. It has solutions for online payment authentication, Web/Portal authentication, and VPN. Although the Web SSO market had \$200 million in revenue in 2000, the better market is the transactional security market. The transactional security market will be in the forefront of ecommerce business enablement. IDC estimates that this market had revenue of only \$148 million in 2000; however, it will grow to over \$2 billion by 2005.

### **Essential Guidance**

The provision of a lightweight, easy-to-use means of protecting digital identities will create value for those transacting business on the Internet, but also for those charged with protecting access to Web-based resources. The benefits will appear in the form of increased transaction levels, reduced risk and fraud exposure, and lower deployment and operational costs. Arcot Systems is one of the companies with an innovative solution that will enable the ultimate realization of the Internet as a safe and reliable venue for business.

To make this promise a reality, Arcot Systems has been working with partners to get the technology fielded as widely as possible. It has a relationship with VeriSign. The company has worked to make its products fit within ecommerce infrastructures, such as Identrus, SWIFT, and MasterCard SPA. Additionally, the company has been working closely with Visa to codevelop the 3-D Secure protocol. Visa has selected Arcot TransFort for its Verified by Visa service, which enables card-issuers to confirm a cardholder's identity to an online merchant during the checkout process. This system reduces online fraud and allows for online transactions to be considered card-present. TransFort has been selected by card processors and service providers, such as First Data Resources, Certegy, Sistema 4B, WorldPay, and CyberSource, and has been deployed at over 20 banks and 50 merchants around the world.

Arcot has also entered into relationships with hardware vendors Compaq and Sun Microsystems. These companies will package the Arcot software in hardware solutions for sale to merchants and financial transaction processors.

### ***IDC Analysis***

Arcot Systems is in a strong position to capitalize on the need for transactional security solutions where large communities of customers and partners, connected only through a browser, make strong user authentication a necessity. Arcot's products provide an end-to-end platform for strong user and transaction authentication for payment systems, Web-based services, business portals, and VPN environments. The key advantage it has is that the Cryptographic Camouflage technology eliminates the need for hardware devices and their associated card readers. Arcot's products combine the security of hardware solutions with convenience and usability of username/password.

*Arcot Systems has developed an attractive set of products that reduce overall costs and enhance the usability and convenience of strong authentication for its customers without compromising the level of security they receive.*

IDC believes that Arcot Systems has developed an attractive set of products that reduce overall costs and enhance the usability and convenience of strong authentication for its customers without compromising the level of security they receive. The company has leveraged its technology through the use of partnerships. Although a small company, Arcot Systems has partnered with some of the biggest players in the ebusiness arena. IDC believes that Arcot Systems is well positioned to be an important player in the transactional security and authentication markets, with a focus on financial services, healthcare, and enterprise customers. Just as the future of PKI lies in greater transparency, ArcotID will also become an almost invisible component. Already, with the Verified by Visa program, consumers are using Arcot Systems technology without knowing the name or the underlying technology.

## Learn More

### ***Related Research***

- *eCommerce Is Here to Stay: Worldwide Internet Usage and Commerce Forecast and Analysis, 2000–2005* (IDC #26113, December 2001)
- *Internet Security Software Spending Opportunity by Vertical Market, 2000–2005* (IDC #25797, October 2001)
- *Worldwide Security 3As Software Market Forecast and Analysis, 2001–2005* (IDC #25668, October 2001)
- *Who Are You — The Western European Market for Security 3A Software* (IDC #IS04H, October 2001)
- *XML and Security 3As: The Universal Translator or Tower of Babel Incarnate?* (IDC #25612, September 2001)
- *Security Underpins Strategic eBusiness* (IDC #AU18110H, September 2001)
- *Transactional Security = eBusiness Enablement* (IDC #23895, February 2001)