

## COVER STORY

April 2001

REACH OUT AND ID SOMEONE

ACCESS CONTROL

BY MANDY ADDRESS

For one ASP, tokens provided the best means of authenticating its VPN users.

The benefits of virtual private networks (VPNs) are obvious, especially with the proliferation of home DSL and cable-modem connections. Remote users can access corporate network services and resources with the same efficiency and functionality as if they were in their home office. Business partners can connect to each other's networks, allowing for sharing proprietary information on joint projects. For organizations employing VPNs, the technology helps improve productivity through an inexpensive conduit.

The problem for many organizations is finding an efficient, affordable and scalable means of authenticating VPN users. Sure, there are many authentication solutions on the market, but not all provide the functionality and ease of use that facilitate user acceptance. Organizations want their VPN connections secure, but realize the security is only as strong as its ability to deploy a system, maintain it and have users consistently employ it.

Finding a feasible authentication solution was the problem facing a San Francisco-based application service provider (ASP) that is designing a merchandise management application to help retailers with inventory planning and management. The startup installed a new firewall/VPN appliance to enable its 75 employees to telecommute and access network resources while traveling. The company anticipates doubling in size over the next year and would eventually like to expand its VPN capabilities to clients and business partners. Like many growing IT businesses, this company realized it needed a two-factor authentication scheme that could provide reliable security, expand with its growth, be easily implemented, and be easy to use by employees and clients--all without breaking its bankroll.

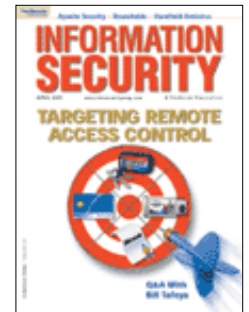
This is where I came in. The company hired me to evaluate various authentication solutions and recommend one that best fit its current and future needs. Under consideration were tokens, certificates, biometrics and smart cards--the usual fare in today's marketplace. Specifically, the company was considering an RSA SecurID (ACE Server 4.1) token, Microsoft's Certificate Server (included in Windows 2000), ActivCard Gold smart cards and Ethentica (MS3000 and USB2500) biometric devices.

While any one of these systems would provide the effective VPN authentication, the company's IT managers wanted a solution that was cost effective (no more than \$100 per user), easy to install and deploy, user friendly, simple to manage, reliable, scalable and included dependable back-up functions.

### The Operating Environment

Identifying the best authentication solution meant evaluating the company's existing IT infrastructure and resources. Its environment is entirely Windows 2000-based, running an MS IIS Web server and a Web Logic application server with an Oracle database. Protecting the network of its corporate office is a NetScreen-10 firewall/VPN gateway, while a Cisco PIX/3000 VPN Concentrator is used at its co-located ASP facility. In some cases, evaluating a VPN authentication solution would incorporate a review of additional servers, but the company has a spare system that made this step unnecessary.

After analyzing the capabilities of the company's NetScreen-10 VPN gateway, I discovered it only supported certificates for VPN authentication. (Recent releases of the product do provide the ability to use authentication through VPN tunnels.) To analyze all options, we decided the company could use a pre-shared secret for VPN authentication and move the two-factor



Issue Archives

Subscribe/  
Change Address  
Int'l Subscriptions

Infosec Jobs

Editorial

Editorial Calendar  
Contact the Editors  
Staff Biographies

Vendor Links

Happenings

Advertising Info

Rate Card  
Editorial Calendar  
Magazine Comparison  
Testimonials  
Internet Opportunities  
Contact a Sales Rep  
BPA Statement  
List Rental Info  
Reprint Info

Security Wire Daily

Back/Missing Issues

About/Contact Us

Directions

Privacy Statement

Security Wire Digest

Read Current Issue  
SWD Archives  
Subscribe to SWD

Home



[Read the wireless Security Wire Daily!](#)

authentication to the Windows domain, so my client may need additional software and tools for its selected solution. Under the company's evaluation criteria, it was clear from the start that biometrics were too expensive and so were eliminated from the analysis (see sidebar).

There are several ways to implement the remaining options. Smart cards can store either digital certificates or just normal Windows logon information. My client preferred not to combine options, so digital certificates were analyzed as a stand-alone authentication technology. If digital certificates won the preliminary analysis, they would be further analyzed for possible use with smart cards.

#### ActivCard Gold Smart Card with ActivPack

ActivCard Gold provides Windows domain authentication by storing a static user password on a smart card, and presents the information through an interface similar to an ATM card. The user enters a PIN to access the information on the card. The Quick Password feature allows the user to drag and drop static passwords from the smart card to any application.

ActivPack with ActivCard Gold allows users to use dynamic passwords and still use the ActivCard Gold Quick Password feature to drag and drop dynamic passwords. The ActivPack server randomly generates a static Windows password for the user, uses a system API to update the domain with the new password, and stores the encrypted password in the ActivPack server database.

When a user logs into the domain, the ActivCard Gold smart card generates the dynamic password internally and passes it to the ActivPack server. The ActivPack server validates the dynamic password.

If everything checks out, the ActivPack server retrieves the static password and sends it to the ActivCard login client. The login client sends the credentials to the Windows domain to complete the authentication process.

The beauty of using smart cards is that the logon process is transparent to the user. Just as with a bank machine, the user cannot access the system without his or her card. Once the card is entered, the user only has to enter a PIN and the system takes over from there. ActivCard can also be configured to lock out a user after a set number of unsuccessful login attempts. Once this occurs, an admin must unlock the card before it can be used again. The user may not be able to access necessary resources during this time.

#### RSA SecurID

SecurID tokens are essentially one-time passwords for user authentication and can be used to authenticate to a Windows domain. The time-synchronized SecurID card has an LCD screen that shows a string of numbers that changes every minute. An agent is required on each system and an ACE/Server resides on the network.

When network access authentication is enabled on a domain controller, users who attempt to connect to protected resources are asked for RSA SecurID credentials. Users' credentials are checked to determine if they have previously authenticated with SecurID and if the credentials are still valid. A successful return from the authentication filter indicates the RSA SecurID authentication passed inspection, and allows the user to proceed to login process.

If a failure is returned, which will happen if a user is accessing the resource for the first time, the user is prompted for the Passcode--a PIN plus a dynamic number generated by the card. The agent then sends the authentication request over the network to the RSA ACE/Server, which determines the validity of the Passcode. A validated Passcode will grant a user network access.

#### Microsoft Certificate Server

Microsoft provides built-in support for certificate authentication in Windows 2000. To use this functionality, the Extensible Authentication Protocol (EAP) must be enabled, a relatively simple process.

The Windows 2000 system employs a mutual authentication process, whereby the user's computer and the network server present their certificates to each other. A public key to verify the user's digital signature is contained in a trusted authority root certificate stored on the user's computer. The root certificates are the basis for certificate verification and should be supplied only by a system administrator.

While the use of certificates is fairly simple, the deployment and implementation process is anything but easy. Creating and implementing the necessary processes and procedures for key and certificate management is laborious and time consuming.

### Cost

Given the \$100-per-user cap, cost was a critical factor in the evaluation process. The company wanted a solution that would provide maximum efficiency without burdening it or its clients with exorbitant deployment costs.

Microsoft's Certificate Server is the least expensive option because the software and server are included with Win2K. The only real cost involved with this solution is the labor needed for designing and deploying a PKI process and educating users on its functionality. While my client didn't need additional equipment, the cost for adding hardware and software for this solution could be substantial. Even though it's difficult to quantify, the deployment costs could average as much as \$150 to \$200 per user.

Another thing to consider: Managing the certificate life cycle can be a costly and time-consuming process. The cost of managing the system can increase over time as an organization adds new users, revokes privileges and issues new keys and certificates to existing users. This cost can be especially burdensome if you have a high number of users with lost or compromised keys.

While my client was already using Win2K, an organization needing to upgrade before certificate deployment would incur substantial costs for purchasing and deploying the software. My client selected Microsoft's Certificate Server as an option because it was already running a Win2K system. A company still running Windows NT might want to consider other certificate options, such as VeriSign or Entrust.

SecurID costs approximately \$75 per user, plus \$9,000 for the ACE/Server software for around 100 users. ActivCard Gold runs about \$95 per user, which covers the user's card and a smart card reader. The ActivPack server for dynamic passwords costs about \$5,000.

### Installation

The company wanted to avoid a long and difficult deployment of an authentication solution, so ease of installation was an important factor. While most of its employees are based in the San Francisco area, managers knew installation would be critical when the company expanded its VPN access to clients.

Again, Microsoft's Certificate Server proved the simplest to install and easiest to integrate with the Win2K logon process. Installation is as simple as selecting certificate services in the "Add/Remove Programs" application. Once the certificate service is activated on a Win2K server, admins cannot rename the system or change many of its configurations. Since certificate support is built into Win2K, there's no need to install additional software agents.

Even though the technical installation is simple, rolling out the procedures to have all users request and receive their certificates may complicate the process. Additionally, the installation process may not be quite as simple for those upgrading to Windows 2000.

SecurID and smart cards are more complex to integrate with Windows, but RSA and ActivCard provide tools to help with this process and make it as seamless as possible. In my experience, the SecurID installation is a little more complex than ActivCard, but the manuals provide excellent help.

While ActivCard is a relatively simple system for users to operate, it requires installation of client software and a smart card reader on every system, which can be time consuming and expensive. Further complicating the deployment is the need to initialize each smart card individually. Once that's done, the ActivPack server must be installed and configured to use the Passcode function. On the plus side, ActivCard is relatively simple to administer once the deployment is complete.

SecurID is a little more complex to install and configure than ActivCard. The ACE/Agent isn't very difficult to install, but the ACE/Server deployment is made difficult by numerous configuration options. However, token initialization is a straightforward process since RSA configures them at the factory and sends a floppy disk with the necessary data for activation and integration.

## User Friendliness

Strong security is the ultimate goal, but implementing an unfriendly authentication solution will impede deployment and make the system less effective for end users. The company wanted a solution that was easy to use, but still provided maximum security. The clear winner in this category is SecurID.

SecurID is easiest for users to adopt and understand since all they need to do is enter the number displayed on the token. This system also provides administrative safeguards--such as setting an account lockout after a set number of unsuccessful login attempts. Admins can also issue temporary passwords to users who lose their tokens.

Smart cards, such as ActivCard's, are well understood by users and easy to use for network access. However, users need to install smart card readers on their home computer systems, and traveling employees need to cart around a reader if it isn't built into their laptops. Once installed, users tend to feel burdened by the need to keep track of their smart cards and readers. The administrative headache of helping users install and maintain smart card readers didn't interest the company.

This is not to say ActivCard isn't a viable option. The interface looks very similar to an ATM machine, so users are generally comfortable with the technology. If a user enters the wrong PIN six times, the account is locked out until it's reset by the network admin.

As for Microsoft's Certificate Server, it's relatively easy to import certificates into the user's certificate store, but this system doesn't provide the two-factor authentication or the physical device my client sought. Both shortcomings can be overcome by using smart cards with the certificates, but this wasn't appealing to the company's IT managers. Short of issuing company-owned laptops to employees, tracking and protecting certificates on multiple systems--particularly employee's personal computers at home--is also not very practical. The company wasn't prepared to issue laptops to all employees to allow them to use only one system.

In addition, users are often confused by certificates and don't understand their purpose in the security infrastructure.

## Management

Smart cards, certificates and tokens are fairly equal in the management arena. Each provides centralized management and multiple configuration options for customizing security. Common management functions that should be included are intuitive administrator GUIs (either Java, Web-based or stand-alone application), the ability to easily add and remove users, auditing and remote management.

SecurID requires administration for tokens that get lost, misplaced, forgotten, locked out, out of sync, etc. ActivCard requires a high level of management for lost cards. Certificates must be revoked and reissued when they expire or are lost or compromised. And, with certificates, admins must maintain a list of revoked certificates (Certificate Revocation List or CRL) to ensure they aren't used again.

In general, certificate protection requires the development of strong security procedures to validate certificate requests and protect the private key to ensure it's not compromised. Procedures should be in place for the admin to respond quickly to a reported compromise by revoking the certificate and issuing a new one. Microsoft provides several tools, such as the Windows 2000 Resource Kit (certutil.exe and dsstore.exe), to help with the certificate management. But, without proper resources or knowledge base, my client wasn't prepared to deploy a PKI system.

## Reliability

While the three authentication solutions have fairly equal performance reliability, certificates have a few issues when it comes to defending attacks. Overall, ActivCard stands out because of its dependable operations and its resilience to attacks. Smart cards, in general, are a proven authentication method since users must use a smart card and a password to access the system. Without the card, reader or PIN, it's very difficult for an attacker to compromise the system.

This is not to say SecurID tokens don't offer a plausible authentication solution. This technology is reliable, but it's vulnerable to performance problems if the client's token and

ACE/Server fall out of sync. Maintaining accurate system time through Network Time Protocol (NTP) is the best solution for this problem.

With Microsoft's Certificate Server, the certificate store doesn't provide the same level of reliability as either SecurID or ActivCard. While reliable in performance, the system is vulnerable to exploitation should someone compromise the user's computer. Keystroke loggers could capture the user's certificate password and use it to gain access to network resources. With a smart card or SecurID, this attack isn't as feasible.

### Scalability

Two issues faced my client in the deployment of an authentication solution: avoiding bottlenecks at the VPN gateway and minimizing the administrative support needed for each new user. The company I was working with wanted a system that was scalable to its current and future needs.

It became apparent that scalability wouldn't be an issue with certificates, tokens or smart cards. RSA claims SecurID can support 100,000 users on a single ACE/Server. Even with the company's immediate expansion plans, it would come nowhere close to the SecurID serviceability limit. As far as scalability goes, SecurID's large capacity made it a feasible solution for my client.

Microsoft's Certificate Server and ActivCard's ActivPack server can also easily handle the number of users my client will be supporting. While the systems can easily handle many users, this also complicates the physical administration. With smart cards, additional readers must be purchased and installed on all systems used by users. With SecurID, admins need to purchase more tokens and manage the user base. The costs of providing these products and services to the user can increase dramatically as an organization grows. With no clear distinction separating these solutions, it was evident that all would work equally well in my client's environment.

### Backup

Without a proper backup solution, any problems with the authentication server--whether due to accident or malicious attack--can be devastating. If an organization loses its entire user database and doesn't have a backup, it'll need to add all users to the system again, reissue credentials, tokens, cards, etc. This process can be expensive, time consuming, and impede an organization's operations if users aren't able to access necessary resources while the authentication problem is being corrected.

Of the three solutions examined, only SecurID has live backup capabilities, setting it apart from ActivCard and the certificate server. The system can be configured with a slave ACE/Server for hot backups. With this setup, if one system goes down, there's a backup server in place to immediately take over authentication functionality.

Microsoft's Certificate Server has built-in services that back up all certificates. Additionally, a tape backup of the certificate server would provide the ability to completely restore the certificate server in the event of a problem. Tape backup is also the best solution for the ActivPack server.

While tape backup is a viable solution, it requires additional hardware, software and administration. Backup schedules must be created, tape rotation and off-site storage must be set up, and administrator activities need to be coordinated to have an effective backup strategy. With SecurID, all an organization needs is a second server running the ACE/Server software.

And the Winner is...

After careful analysis of the three options, the San Francisco startup chose the RSA SecurID (ACE Server 4.1) token. While impressed by the capabilities and functions of the other products under consideration, the company concurred with my analysis that the token solution best fit its needs criteria.

By deploying SecurID, the company wouldn't have to worry about installing card readers on all its remote systems, employees' personal computers or their clients' systems to support the ActivCard solution. Using SecurID would also avoid the education process and management difficulties of implementing a certificate-based system.

Since it's essentially a server-based application, the RSA system is relatively simple to install. Give the users a token, and all they have to do is enter the proper access code when logging into the network. Tokens have a relatively short ramp-up time since users are usually familiar with the technology. It's also easy to scale up since the server can handle a large number of users.

For this company, the RSA SecurID token also provided the best management options. With its centralized management capabilities, administrators can assist remote users having difficulty authenticating, issue temporary passwords and add new users when needed.

It's important to note that certificates, smart cards and biometrics all have their place in an authentication infrastructure. What works for this company may not work for every organization, so it's important to exercise due diligence in evaluating and selecting an authentication solution.

Without a proper backup solution, any problems with the authentication server--whether due to accident or malicious attack--can be devastating. If an organization loses its entire user database and doesn't have a backup, it'll need to add all users to the system again.

Certificates, smart cards and biometrics all have their place in an authentication infrastructure, so it's important to exercise due diligence in evaluating and selecting an authentication solution.

MANDY ADDRESS, CISSP, SSCP, CPA, CISA, ([mandy@arcsec.com](mailto:mandy@arcsec.com)) is founder and president of ArcSec Technologies, a security consulting firm focusing on product and technology analysis.

## FINGERING BIOMETRICS

In the 1960s, science-fiction icon Gene Roddenberry--father of the Star Trek franchise--could only imagine a time in the 23rd century when members of a futuristic society could use their hand and voice prints much the same as we use house and car keys today. Roddenberry lived long enough to see the biometrics technology he conjured for the galactic TV series coming into reality--about 200 years ahead of his prediction.

Just as Capt. James T. Kirk used his retina and voice print to access the starship Enterprise's computers, ordinary computer users today are using compact and easy-to-operate biometric solutions to authenticate network resources. Fingerprint readers, voice recognition software, facial identification cameras and retina scanners are among the options now available for desktop and laptop computers.

Biometrics was one of the technologies under consideration by a San Francisco-based ASP for its VPN authentication solution. When the company hired me to evaluate the various technologies, it set rigid parameters to measure each product--among them cost, ease of deployment, scalability and ease of management. While biometrics would have fit nicely into the company's existing infrastructure, the technology was taken out of consideration because it couldn't meet some of the basic standards.

Under consideration was Ethentica's Ethenticator Touch Verification Card (MS3000 PCMCIA version for laptop users and USB2500 version for desktop), a biometrics fingerprint reader that plugs into a computer and provides access control, a secure screen saver and Web-site password protection. The cost immediately knocked biometrics out of consideration. The company wanted to spend no more than \$100 per user, and biometrics would have run between \$120 and \$175 per user.

Reliability was also a major consideration. While biometrics dependability continues to improve, it still suffers from the effects of environmental factors--i.e., sweaty or wet fingers. The system can default to a password process should the biometrics fail, but could result in a user being locked out of the network should he enter the incorrect PIN too many times.

Biometrics also failed to meet the benchmark for deployment and ease of installation. Just as readers would have to be installed on every computer for a smart card system, Ethentica's verification card would have required installing plug-in ports on every computer--the company-owned, as well as employee-owned home systems and business clients' systems.

While fingerprint readers are relatively simple to use--plug it in and put your finger on the optic--the system isn't exactly user-management friendly. Once the system has been installed on a user's or client's remote computer, it's up to them to manage the biometrics device. For my client, it would take more time and resources to support a biometrics

deployment than the company was willing to invest.

On the plus side, Ethentica's SecureSuite (sold separately for domain access) application would have provided easy centralized administration. The management application makes it simple to add new accounts, convert legacy accounts and remove users.

Even though biometrics is a viable authentication solution, it remains an immature technology that is only suited for select environments. Perhaps, as the technology advances, the costs will come down and deployment will be made simpler, bringing it within reach of organizations similar to my client.

-Mandy Address

## CASE STUDY

### ACCESS TO COST SAVINGS

Role-based access control systems can save organizations time and money.

BY BRIAN KROPP & MICHAEL GALLAHER

Access control within an organization's computer network is needed to control the actions, functions, applications and operations of legitimate users and to protect the integrity of the stored information. The effectiveness of access control systems can be measured on two criteria: reliability of security and ease of administration.

Role-based access control (RBAC) is a relatively new approach that maps to organizational-specific structures, improving security and reducing administrative cost by granting users access to applications, information and networks based on their role and not their individual identity. RBAC technology can replace other access control systems, such as access control lists or discretionary access control.

RBAC has many operational benefits, one of the most significant is cost savings to an organization. Firm figures of RBAC cost savings are unavailable, but a survey of Information Security readers conducted by the Research Triangle Institute (RTI) on behalf of the National Institute of Standards and Technology (NIST) provides a glimpse of financial benefit this new technology can produce.

What is RBAC?

RBAC is a software-based tool that can be incorporated into existing software tools and improve overall security by simplifying the duties, tasks and administrative responsibilities of network admins. Access can take several forms, including restricting the viewing, use and altering of specific data.

While previous network access control systems have provided these functions, RBAC has two unique advantages. First, because RBAC is based on the worker's role rather than the user's identity, direct and indirect administrative costs are greatly reduced. By assigning individuals to predefined roles, the administrative process of establishing privileges is streamlined and management time for reviewing privilege assignments is reduced. Second, RBAC provides greater security than competing technologies because it prevents users from obtaining inconsistent or incompatible privileges that can enable access violations.

The traditional approach to controlling access to information and network resources is to establish specific permissions for each user. While effective in a static environment, this approach is often difficult to manage in dynamic environments, where users enter and leave, or change positions within the organization. The constant stream of changes requires frequent updating of access permissions, an often time-consuming, expensive and error-prone process. A common security lapse with this approach is admins not making timely permission updates, enabling unauthorized users to access restricted data.

RBAC addresses these management issues by basing access on a user's role--or job responsibilities--rather than customizing access for each individual. For instance, everyone in a company's accounting department will be given access to financial data and systems, but not to the production scheduling applications.

On the surface, basing access on job descriptions may seem a bit restricting, but RBAC allows for granting groups multiple access permissions and even the ability to allow specific individuals elevated access privileges. Applying this to our previous example, the accounting

department staff would have access to financial systems and data, but their managers could also be granted access to human resource files and marketing projections. Roles can also be set up based on locations, projects and management level.

The efficiency and cost savings come from the diminished administrative need in maintaining a RBAC system. Employee turnover and assignment changes make it difficult to keep up with the constantly changing human resources landscape. That's not the case with roles, which usually don't change too often. By only having to add and remove users from role groups, the organization can cut down on the administrative costs and reduce the potential for error.

RBAC has the potential to be used in almost any organization that uses a computer network to limit access to particular pieces of information. Industries that will especially benefit from RBAC are those for which information security is a key, such as banking, health care, government, software development and the military.

A recent report by SETA Corp., sponsored by NIST, asserted that organizations with certain staffing, data and organizational characteristics could reap tremendous benefits from deploying a RBAC system. These characteristics reflect the common problems found in many IT-dependant organizations: tremendous demand for services clashing with limited resources. According to SETA, organizations with large staffs with high turnover rates, limited security resources, stable organizational structure and application, and maximum control over IT resources and data would benefit the most from a role-based access system.

### Quantifying RBAC Benefits

Based on an ongoing RTI study, firms that implement a RBAC system yield two major benefits: reduced administrative overhead and improved employee productivity. With access based on roles, admins aren't hampered by the laborious task of updating individual user privileges. Consequently, employees can gain faster access to systems critical to their jobs. To investigate the potential magnitude of these benefits, RTI compiled the responses of more than 100 Information Security readers on the administrative costs associated with various access control systems.

Organizations using RBAC reported significant timesaving over conventional user-based access control systems in assigning privileges to new users, and slightly better ability to change, modify and terminate user privileges. Applying the number of times these tasks are performed on a daily basis and the number of employees in an organization, we calculated that a RBAC system could save an organization 7.01 minutes per employee, per year in administration functions. Seven minutes doesn't seem like much, but it takes on great significance when combined with the average hourly salary of an IT admin-\$59.27 per hour on average. The annual cost savings ranges from \$6,924 a year for organizations with 1,000 employees to \$692,471 for organizations with 100,000 employees.

The cost savings are further amplified when combined with the reduced employee downtime. If new and transitioning employees receive their system privileges faster through a RBAC system, their productivity is increased. Survey respondents said their average downtime for new employees while waiting for system access privileges was 26.4 hours with non-RBAC systems and 14.7 hours with RBAC systems--resulting in an overall change in average downtime of 11.7 hours per new employee. Assuming the average employee hourly wage is \$39.27, the annual employee turnover rate is 13 percent and the annual growth rate is 3 percent, the annual productivity cost savings yielded by a RBAC system ranges from \$75,000 for organizations of 1,000 employees to \$7.4 million for organizations of 100,000 employees.

### Improved Security

While security is a chief concern of many organizations, management more often sees it as a drain on financial resources than as a benefit to the bottom line. This perception persists until the inevitable happens--the organization suffers from an insider security lapse. Various surveys, including those conducted by Information Security, have found that a significant number of organizations have experienced an insider security lapse, costing an average of about a quarter-million dollars per incident.

Role-based access control systems are designed to minimize the potential for inside security violations by providing greater control over users' access to information and resources. We presume the enhanced security provided by RBAC systems would result in further cost savings, but our survey respondents were unwilling to share information on the number, if any, and costs of their security violations. However, some respondents, without providing specifics, did indicate that RBAC systems reduced the number of security violations in their organizations.

Obviously, the administrative savings, downtime savings and security benefits derived from RBAC systems will vary based on the size of an organization and its industry. Based on our calculations, medium- to large-sized organizations would yield a quicker ROI from deploying a role-based system, since the savings increase with the number of users on a system. But, as the survey shows, organizations of all sizes can yield a significant return on investment--both in direct and indirect costs--by deploying a role-based access control system.

**TABLE 1: ESTIMATED TIME (IN MINUTES)  
REQUIRED FOR ACCESS ADMINISTRATIVE TASKS**

<b>TASK</b>	<b>RBAC</b>	<b>NON-RBAC</b>	<b>DIFFERENCE</b>
Assign existing privileges to new users	6.14	11.39	5.25
Change existing users' privileges	9.29	10.24	0.95
Establish new privileges for existing users	8.86	9.26	0.40
Termination of privileges	0.81	1.32	0.51

BRIAN KROPP ([bkropp@rti.org](mailto:bkropp@rti.org)) is a research economist at RTI and specializes in the economics of software development and technology policy.

MICHAEL GALLAHER, Ph.D. ([mpg@rti.org](mailto:mpg@rti.org)), is the director of RTI's Technology Economics and Policy program, and conducts economic impact assessments of new and emerging technologies.

[HOME](#)

# ASSESSING VPN

Company/Product	CATEGORY/WEIGHT Cost/10	PP=POSSIBLE POINTS CATEGORY/WEIGHT PP: 100	CATEGORY/WEIGHT Installation/7	PP=POSSIBLE POINTS CATEGORY/WEIGHT PP: 70	CATEGORY/WEIGHT User Friendliness/8	PP=POSSIBLE POINTS PP: 80
<b>RSA SecurID</b> <a href="http://www.rsasecurity.com">www.rsasecurity.com</a> 	<p>The least expensive token technology of those compared, but not the cheapest solution overall.</p> <p>Score: 7</p>	70	<p>ACE/Agent and ACE/Server are a little complex to install and configure, but integration with Win2K is relatively easy.</p> <p>Score: 7</p>	49	<p>Technology is familiar to most users and requires little training.</p> <p>Score: 9</p>	72
<b>ActivCard Smart Card</b> <a href="http://www.activcard.com">www.activcard.com</a> 	<p>Smart cards are still a little expensive for average-sized companies to implement for network access control.</p> <p>Score: 6</p>	60	<p>Initialization is time-consuming. Otherwise, installation and integration are very straightforward.</p> <p>Score: 7</p>	49	<p>While most users are familiar with the form factor, they aren't willing to keep track of both the smart card and the reader.</p> <p>Score: 8</p>	64
<b>Microsoft Certificate Server</b> <a href="http://www.microsoft.com">www.microsoft.com</a> 	<p>The cheapest of the four options when comparing straight acquisition cost. However, the required processes and procedures may add a significant cost when comparing all required resources.</p> <p>Score: 9</p>	90	<p>Installation and integration are very easy, since everything is included in Win2K.</p> <p>Score: 8</p>	56	<p>Users are still mystified by certificates. Additionally, keeping track of certificates across multiple systems is often difficult.</p> <p>Score: 6</p>	48
<b>Ethentica</b> <a href="http://www.ethentica.com">www.ethentica.com</a> 	<p>While the cost of biometric devices has decreased recently, they are still the most expensive authentication option.</p> <p>Score: 5</p>	50	<p>Installation and integration are very simple and user friendly. Ethentica provides great tools to help with the Windows integration process.</p> <p>Score: 8</p>	54	<p>The SecureSuite software is intuitive and easy to use for the average user. (Plus, users just might feel like James Bond when using it!)</p> <p>Score: 9</p>	63

**FOOTNOTE:**

Each category is weighed based on the criteria of the author's client's criteria. The individual category scores are multiplied by the weighted score to arrive at the final score.

# ACCESS CONTROL

CATEGORY/WEIGHT	PP=POSSIBLE POINTS	CATEGORY/WEIGHT	PP=POSSIBLE POINTS	CATEGORY/WEIGHT	PP=POSSIBLE POINTS	CATEGORY/WEIGHT	PP=POSSIBLE POINTS	Verdict	TPP=TOTAL POSSIBLE POINTS
Management/6	PP: 60	Reliability/6	PP: 60	Scalability/3	PP: 30	Backup/5	PP: 50		TPP: 450
<p>Centralized management is available. Adding and removing users is simple.</p> <p>Score: 8</p>	48	<p>Reliable technology, but synchronization issues may cause a few headaches.</p> <p>Score: 8</p>	48	<p>Handling 100,000 users on a single server provides more than enough support for most organizations.</p> <p>Score: 10</p>	30	<p>Slave server's hot backup with fail-over capability makes this the top backup solution.</p> <p>Score: 10</p>	50	<p>Best overall solution for this case study. Widely supported, highly scalable, fail-over capable, easy integration and centralized management make administrators happy. Users only need to keep track of an easy-to-use key fob.</p>	367
<p>Centralized management is available. Adding and removing users is simple.</p> <p>Score: 8</p>	48	<p>Smart card reliability is excellent. The only problem is users forgetting their PINs.</p> <p>Score: 9</p>	54	<p>Can scale easily, but the added administration per user makes it a little less scalable than SecurID.</p> <p>Score: 9</p>	27	<p>Backing up the ActivServer with a tape system is effective, but adds administrative overhead.</p> <p>Score: 8</p>	40	<p>A strong solution, but the reader requirement makes this solution less viable than others.</p>	342
<p>Even though centralized certificate management is available, the entire PKI management process isn't easy to implement or understand, especially for a novice.</p> <p>Score: 6</p>	36	<p>Secure certificate storage can be a labor-intensive process.</p> <p>Score: 4</p>	24	<p>Certificates are very scalable, especially if the entire management process is automated.</p> <p>Score: 10</p>	30	<p>As with smart cards, backing up the Certificate Server with a tape system is effective, but adds administrative overhead.</p> <p>Score: 8</p>	40	<p>This is the least expensive option, but certificates require the development of complex policies and procedures. Additionally, this technology confuses a lot of users.</p>	324
<p>Centralized management is available, but you must purchase an additional server.</p> <p>Score: 7</p>	42	<p>The fingerprint scanner was very reliable in testing. Finger must be dry before placing it on the scanner.</p> <p>Score: 8</p>	48	<p>While the server can handle a large number of users, managing and supporting many biometric devices places an additional burden on support staff.</p> <p>Score: 7</p>	21	<p>A tape system is the best backup for this technology, but it adds administrative overhead.</p> <p>Score: 5</p>	25	<p>Technology is unique, but cost is too high. Problems arise when client laptops don't have open PCMCIA slots. As with a smart card reader, the USB finger scanner is cumbersome in mobile environments.</p>	303