When the year 2000 was nearing its end, Taipei County Government (www.tpc.gov.tw/english/index.htm) initiated a project to greet the millennium with a new approach to an old problem: managing users’ access to network resources. The project was both reactive and proactive, with the intent being to solve existing and anticipated problems with managing user accounts and protecting network resources.

As planned, security project manager Jang-Ming Young began the project by researching Lightweight Directory Access Protocol (LDAP)-compliant directories. Taipei County Government hoped an LDAP-compliant directory would provide the foundation for a complete access-management solution. As Young searched the web, he found multiple documents pointing to Novell eDirectory as the LDAP-compliant directory of choice. As a result, Young contacted a local Novell partner—and the rest, as the cliché goes, is history.

Today, Taipei County Government runs a Novell access and security solution and has completed the first phase in its two-phase project. (Novell access and security solutions enable organizations to securely manage access to applications, databases, and platforms for all types of clients. For more information, see “Rethinking Security: Seven Steps to Tighten Network Security” on p. 6. For more information about the project, see “The Project Plan” on p. 28.)

THE NETWORK SITUATION

As the governing body for the largest of 16 counties in Taiwan, Taipei County Government has a sizable workforce. (See “Taipei County” on p. 26.) More than 1,700 employees work in the 27 departments within the adjacent pair of Taipei County Government buildings that are located in Ban-chiao, about 10 km (8.5 miles) southeast of Taipei city. (See Figure 1.)

The employees in these departments use approximately 1,500 workstations. Two hundred of these workstations are not connected to Taipei County Government’s IP-based 100BaseT Ethernet LAN. The remaining 1,300 workstations are Windows 2000/NT/98 clients—virtually all of which are desktop PCs, with the exception of approximately 100 laptops.

Before implementing the Novell access and security solution, the Taipei County Government network consisted of four servers:

- One Sun Solaris server that also ran iPlanet Messaging Server which was integrated with Netscape Directory Server running on the same server
- One Windows 2000 server, which ran a custom-built Certificate Authority (CA) that was integrated with Netscape Directory Server and ran on top of Microsoft Internet Information Server (IIS)
- Two Windows NT 4.0 servers with Service Pack 4, which ran several commercial and custom applications

THE PROBLEM

The problem was that to access applications and data—even the most confidential information—employees needed to enter only a password. Taipei County Government recognized that password-protection alone does not adequately protect important and confidential resources. For example, if an employee guessed
an MIS specialist's password, this employee could have accessed other employees' e-mail messages, created or removed user accounts, and modified user privileges— to name only a few of the possibilities.

Compounding this problem was the fact that each of the 1,700 employees had multiple accounts, including two frequently used accounts: one account for the Netscape Directory Server and one account for Windows NT domains. Two frequently accessed accounts per user (not to mention their less-frequented accounts) was one account too many and caused the usual set of problems.

For one thing, employees had to enter a different set of credentials every time they switched between the applications in the Windows NT domains and the iPlanet messaging application. Aside from being annoying, this practice was inefficient and took time.

Admittedly, entering credentials and waiting to be authenticated takes only seconds—perhaps as few as ten seconds. However, even ten seconds adds up quickly when you have 1,700 employees entering credentials as many as three times a day. In fact, do the math using the hypothetical values of ten seconds and three times daily. Given these values, you can guestimate that Taipei County Government employees were collectively spending approximately 71 hours per week doing nothing more than entering credentials and waiting to be authenticated.

In addition to costing users time, two user accounts per employee cost the MIS specialists time. As a network administrator, you’re probably not surprised to learn that Taipei County Government employees frequently forgot one or both of the passwords to their user accounts. Consequently, the 14 engineers in Taipei County Government’s IS&T department spent more time than they wanted assigning new passwords.

Help-desk issues aside, managing two accounts per user was impractical and time-consuming. For example, to manage access control rights for the Netscape directory, MIS specialists had to use the Netscape Directory Server console running on the Sun Solaris server. To control users’ access rights to resources in the network’s Windows NT domains, the MIS specialists had to use the Windows management application running on the Windows NT Primary Domain Controller (PDC). In other words, to manage user accounts, MIS specialists had to work on separate computers, use different applications, and, most important, understand dissimilar philosophies for setting access rights.

Not surprisingly, the MIS specialists found that the process of creating new user accounts and assigning appropriate privileges sometimes took as long as three days. Clearing accounts belonging to former employees commonly took more than a week. What was more disconcerting than the time involved in clearing accounts was the uncertainty involved: Without a central point of management for user accounts, MIS specialists frequently worried that they hadn’t actually cleared all of the access rights to all of the resources to which a former employee had access.

Despite these problems, when Taipei County Government started its project, managing user accounts was tolerable. However, Taipei County Government was looking ahead. Like most organizations, Taipei County Government anticipated that its network would grow. Taipei County Government drew the logical

Figure 1. Taipei County Government offices are located in Banchiao, which is just 10 km (8.5 miles) southeast of Taipei city. Taipei city is located in Taipei county, which is the largest of Taiwan’s 16 counties.

Please visit our advertiser Ecora at www.ecora.com.
The large of the Western Pacific islands, Taiwan is roughly the size of Maryland and Delaware with a population nearly four times as large. Of the 22.5 million people who live in Taiwan, 3.6 million live in Taipei county alone—the most heavily populated of Taiwan’s 16 counties. Taiwan’s counties include the following: Taipei, Taoyuan, Hsinchu, Miaoli, Taitung, Hualien, Nan’tou, Ilan, and Penghu.

Like every county in Taiwan, Taipei county has its own government headed by magistrates and councillors. Magistrates are elected by popular vote for up to two four-year terms of office, while councillors are popularly elected for four-year terms of office. Taipei county’s December 2001 elections placed 64 new councillors and secured a second term of office for Magistrate Chen-Chang Su.

According to Young, ZEN works for Desktops 3 is “one-tenth the cost [of the competitor’s solution] but ten times more powerful.” (For more information about ZENworks for Desktops 3, visit www.novell.com/products/zenworks/desktops.)

Standardizing on eDirectory
To provide systems integration services, SecureInside initially contracted with UniBiz (www.unibiz.com.tw) and later with Bizwave (www.bizwave.com), both Novell partners. UniBiz was responsible for installing all of the Novell products.
running on Taipei County Government’s network today, with the exception of NMAS. Bizwave contributed to the first half of the Taipei County Government’s access-management project and continues to work on the second half.

To start the project, UniBiz installed NetWare 5.1 (www.novell.com/products/netware5) on two newly purchased IBM xSeries 300 servers. (See Figure 2.) Each IBM xSeries 300 server (www.pc.ibm.com/us/eserver/xseries/x300) is equipped with a Pentium 1 GHz processor, 1 GB of RAM, and an 18 GB hard drive.

Next, UniBiz installed eDirectory 8.5.1 on the NetWare, Windows 2000, and Windows NT servers. UniBiz did not install eDirectory 8.5.1 on the Solaris server because Taipei County Government plans to migrate the Solaris server to Microsoft Exchange 2000. (For more information, see the “What’s Done and What’s Next?” section on p. 33 and the “The Project Plan” sidebar on p. 28.)

Because Taipei County Government runs so many different server platforms on its network, eDirectory is the logical choice for an LDAP-compliant directory on which to standardize. Recently named directory product of 2001 by Network Magazine, eDirectory is the only directory on the market that runs on all major operating systems including NetWare, Windows 2000/NT, and Solaris, as well as Linux, Compaq Tru64, UNIX, Linux, and IBM AIX. (For more information about Network Magazine’s Products of the Year awards, visit www.networkmagazine.com/article/NMG20010413S0005.)

As the cross-platform repository for all identity, policy, and access-control information, eDirectory is the foundation for the Novell access and security solutions. eDirectory is also highly scalable, with the ability to store and manage billions of objects while maintaining fast lookup speeds. (For more information, visit www.novell.com/products/nds.)

Consolidating User Accounts

To consolidate user accounts, UniBiz installed Novell Account Management 2.1 on the NetWare, Windows NT, and Windows 2000 servers. (See Figure 2.) Formerly named NDS Corporate Edition, Novell Account Management 2.1 is an eDirectory-enabled application that simplifies and unifies the management of user profiles on Windows 2000, Windows NT, Solaris, and Linux servers. (For more information about Novell Account Management 2.1, visit www.novell.com/products/nds/accountmanagement.)

SecureInside offers more than systems integration services such as those it provided for the Taipei County Government access-management project. Founded in 1996, SecureInside helps government agencies in Taiwan deploy workflow solutions based on a public-key infrastructure (PKI).

For example, SecureInside helped Taipei County Government set up an electronic document-exchange solution that enables employees to apply, have approved, and follow-up on requests for leave, purchases, and reimbursement (for travel expenses, for example). Over the past five years, SecureInside has expanded this solution to include the Department of Land Administration’s 107 offices and other government agencies as well, such as banks and courthouses within Taipei city and county.

Because SecureInside is a small company, it considers its partners, including Novell, critical to its success. “Novell is an important partner,” says SecureInside senior manager Luke Lee. In fact, Lee adds, Novell products play a major role in all of the solutions SecureInside deploys and helps deploy throughout Taiwan.

Please visit our advertiser Beginfinite at www.beginfinite.com.
The Project Plan

To date, Taipei County Government has completed Phase 1 of its two-phase project to improve and extend access management:

<table>
<thead>
<tr>
<th>PHASE 1</th>
<th>DONE?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consolidate user accounts and enable single sign-on</strong>&lt;br&gt;• Integrate user accounts on Windows NT and Windows 2000 servers with Novell eDirectory 8.5.1 using Novell Account Management 2.1</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Protect network resources through multifactor authentication</strong>&lt;br&gt;• Install Novell Modular Authentication Service (NMAS) 1.0 Enterprise Edition&lt;br&gt;• Integrate Tai-Hao smart card and fingerprint readers with NMAS 1.0</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Enable remote users to securely access the network via Remote Authentication Dial-In User Services (RADIUS) protocol</strong>&lt;br&gt;• Install BorderManager Authentication Services (BMAS) 3.6</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Integrate existing products (such as custom certificate server) with eDirectory 8.5.1</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Integrate custom Electronic Document Exchange application with Lightweight Directory Access Protocol (LDAP)</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Install new Linux server running new web management console and integrate with eDirectory</strong></td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PHASE 2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Extend Novell eDirectory 8.5.1 to entire county network</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Migrate from iPlanet Messaging Server to Microsoft Exchange 2000</strong></td>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FUTURE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Provide online government services to residents of Taipei County through eDirectory-based solution</strong></td>
<td>No</td>
</tr>
</tbody>
</table>

UniBiz successfully installed the Novell Account Management components and also ran the Domain Object Wizard, which transparently migrated all existing NT domains into eDirectory.

Once installed, Novell Account Management 2.1 created accounts in eDirectory for Taipei County Government’s existing Windows NT user and group profiles. Next, Novell Account Management 2.1 made these accounts available to services running on the Windows NT servers through a process called redirection. Basically, redirection refers to a process whereby Novell Account Management 2.1 redirects to eDirectory any user requests for services running on the Windows NT or Solaris servers. (For more information, see “Redirecting to eDirectory Requests for Services in NT Domains” on p. 30.)

By running Novell Account Management 2.1 on the various server platforms, each of the 1,700 Taipei County Government employees now has a single user account in eDirectory. As a result, employees now have only one set of credentials they can use to access all of the network resources to which they have rights—regardless of the platform on which those resources run.

What may be more important is how consolidating user accounts has simplified user account management. MIS specialists now have the luxury of managing only one user account for each of the network’s 1,700 users. In fact, the MIS specialists can complete all tasks related to managing user accounts using a management interface to eDirectory, such as ConsoleOne, eDirectory’s Java-based administrative utility.

For example, when MIS specialists want to assign a new user access rights to applications in the Windows NT domains, they can do so using ConsoleOne. To move a user from one Windows NT domain to another, MIS specialists can again use ConsoleOne (and incidentally, they won’t have to recreate or delete accounts to do so).

In addition to using the ConsoleOne interface to eDirectory, Taipei County Government’s MIS specialists can also use a web management console. This web management console runs on a new Linux server that is running the Apache web server (http://httpd.apache.org). The Linux server also runs Tomcat, a JavaScript Pages (JSP) engine also developed by the Apache Software Foundation (http://jakarta.apache.org/tomcat). (See Figure 2 on p. 26.)

By creating this console, Bizwave enabled MIS specialists to access Taipei County Government’s eDirectory tree and to manage user accounts from any network client running a standard web browser. The MIS specialists can use this web console to perform tasks such as creating User, Group, and Organizational Unit (OU) objects and managing access control lists (ACLs).

Enabling Multifactor Authentication

Novell Account Management 2.1 alleviated the problems of managing multiple user accounts and, to some extent, increased network security. After all, users now have only one set of credentials to memorize and, therefore, are less likely to jot down these credentials as a means of remembering them. MIS specialists can manage user accounts from a central point. As a result, creating new accounts and assigning new access rights take less time. More important, in this context, clearing old accounts is easier—and no longer leaves the MIS specialists worrying that perhaps they have missed something.

Novell Account Management 2.1 clearly provides a better approach to managing user accounts and, thereby, offered the beginnings of improved security. To better protect network resources, however, Taipei County Government deployed NMAS 1.0 Enterprise Edition (www.novell.com/products/nmas).
Novell Account Management 2.1 redirects users’ requests for services running on various platforms to eDirectory. These platforms include Windows 2000 and NT, Solaris, and Linux. For example, to redirect to eDirectory users’ requests for services running on Windows NT, Novell Account Management 2.1 replaces a key Microsoft file (called SAMSRVDLL) with an eDirectory-based file.

On Windows NT, resources are created and managed in a database called the System Account Manager (SAM). Applications that need information from the Windows NT domain make requests to SAMLIB.DLL. These applications include those running on the NT server or on an NT workstation.

SAMLIB.DLL uses Remote Procedure Calls (RPCs) to communicate with SAMSRVDLL. For applications being run on the server, this communication is done internally. For requests originating from a workstation, the RPC requests are sent to the server. After the server RPC receives a request, it is extracted and passed to SAMSRVDLL. SAMSRVDLL then accesses SAM, where the domain namebase is stored and performs the requested operation. (See Figure 4.)

Novell Account Management 2.1 relocates Windows NT domains into eDirectory by replacing the Microsoft SAMSRVDLL file with an eDirectory-based SAMSRVDLL file. All application requests to the domain namebase are then redirected to eDirectory (which can reside on a NetWare server, an NT server, or both). eDirectory stores the User, Computer, and Group objects that take the place of the objects previously used from the domain. (See Figure 4.)

The advantage of this redirection is that all existing applications continue to work without any change. You can continue to use familiar Windows NT tools to manage accounts in eDirectory. eDirectory containers can scale into hundreds of thousands of objects, unlike NT domain objects, which are limited to a few thousand.

NMAS 1.0 enables Taipei County Government to create authentication policies that require users to authenticate to eDirectory using login methods based on any type of login factor (such as passwords, smart cards, or fingerprints). As you can guess, NMAS 1.0 extends the eDirectory schema to allow for storage of additional authentication information, such as personal identification numbers (PINs) and fingerprints. In addition, the NMAS 1.0 Enterprise Edition (as opposed to the NMAS Starter Pack) enables Taipei County Government to create login sequences based on any combination of login factors so that employees have to enter one, two, or three factors to gain access to various network resources.

NMAS 1.0 supports various login methods through several authentication modules that Novell and third-party vendors provide. For example, Novell developed modules that enable users to log in using an eDirectory password or an X.509 v3 certificate. Third-party authentication modules include modules from A cti cCard Inc., Identicator Technology (a division of Identix), RSA Security, SA FLIN K Corp., and V A SCO Data Security Inc. These authentication modules enable security vendors to integrate their authentication devices in an NMAS environment.

To deploy NMAS 1.0, Taipei County Government worked closely with Novell-trained engineers at Taiwan Developer Labs. Taiwan Developer Labs are sponsored by the Ministry of Economic Affairs (MOEA) and the Institute for Information Industry (III), a nonprofit organization chartered to help the Taiwanese government encourage the growth of the country’s information industry. (For more information, visit www.iii.org.tw/portal/english.htm.) Taiwan Developer Labs are also sponsored and supported by Novell Worldwide Developer Support.

Taiwan Developer Labs installed the NMAS server software on the NetWare 5.1 server running the eDirectory master. (See Figure 2 on p. 26.) The engineers from the Labs also installed NMAS 1.0 client software on each of the network’s 1,300 workstations.

Next, Taiwan Developer Labs equipped most of the Taipei County Government network’s workstations with smart card and fingerprint readers.

Integrating Tai-Hao Devices
Taipei County Government chose three authentication devices from Taiwan Tai-Hao Enterprise Co. Ltd. (www.tai-hao.com). A II of the laptops and most of the desktop PCs, according to Tai-Hao representative Jerry Lai, are equipped with Tai-Hao’s Smart Card Reader Keyboard F21KC (www.tai-hao.com/english/product/cardreader.html).

In addition, some of the desktop PCs are equipped with Tai-Hao’s Smart Card Reader F21RC (www.tai-hao.com/english/product/cardkey.html). These smart card readers can read any smart card that supports the International Standardization Organization (ISO) 7816 standard. A few of the desktop PCs are also equipped with Precise Biometrics’ Fingerprint Reader PB100SC (www.tai-hao.com/english/product/finger.html).

Tai-Hao also provided Tai-Hao’s Smart Card Reader Keyboard F21KC and Smart Card Reader F21RC for the Taipei County Government with the following two authentication modules:

• A smart card reader module for the fingerprint reader. Tai-Hao purchased the module for the fingerprint reader from Precise Biometrics (www.precisebiometrics.com), a Swedish company that develops high-level security solutions based on fingerprint verification. Tai-Hao is the sole agent and distributor of Precise Biometrics’ Precise 100 series of fingerprint readers in the Asia region. According to Lai, Precise Biometrics developed the NMAS modules for its Precise 100 series in cooperation with SA FLIN K.

• A smart card reader module for the fingerprint reader. Tai-Hao worked with engineers in Taiwan Developer Labs to develop the III NMAS Smart Card Login Module for the smart card reader and
smart card reader keyboard. "Tai-Hao appreciates Novell's cooperation [on this project] to a great extent," says Lai.

THE SEQUENCE TO SUCCESS

With the requisite hardware and software installed, the Novell-trained engineers from Taiwan Developer Labs worked with Taipei County Government to use several login sequences. Taipei County Government employees are now required to enter up to three login factors—an eDirectory password, a smart card, and a fingerprint—depending on the importance and each resource's relative level of confidentiality.

Setting up these login sequences required first creating Login Method objects in the Login Mthod container—one object for each of the Novell and third-party methods. In this case, the engineers created Login Method objects for each of the following methods:

- eDirectory password
- Tai-Hao smart card reader
- Precise Biometrics fingerprint reader

These sequences are stored as properties of the Login Policy container object. The Novell engineers created the following login sequences:

- eDirectory password
- eDirectory password and smart card
- eDirectory password and fingerprint
- eDirectory password, smart card, and fingerprint

MAKING THE GRADE

Deploying NMA S 1.0 Enterprise Edition enabled Taipei County Government to make use of the NetWare 5.1 graded authentication feature. The graded authentication feature (first included with NetWare 5) tightens security through a combination of grades, security labels, and clearance levels. Basically, graded authentication better protects resources by requiring users to log in using a sequence that matches their security clearance, which must in turn match the grade of the resource they want to access. Naturally, users must also have the appropriate rights.
**NMAS Under Cover**

What happens behind the scenes when a Taipei County Government employee attempts to authenticate to the network’s Novell eDirectory tree? Suppose employee Patrick has just completed the fields on the initial login screen. (See Figure 3 on p. 27.) The NMAS client running on Patrick’s workstation stores the values Patrick enters in the Windows registry. When Patrick clicks OK, the regular Novell client invokes the NMAS client.

On Taipei County Government’s network, the NMAS client establishes a connection with the NetWare 5.1 server that stores the eDirectory master replica, which holds a copy of Patrick’s (and each other employee’s) User object. (See Figure 2 on p. 26.) Using Novell International Cryptographic Infrastructure (NICI), the NMAS client and server create a secure pipe over which they can exchange encrypted authentication information.

The NMAS client next sends a message to the NMAS server. This message indicates all of the login methods that have been installed on this workstation client. Novell assigns numbers to each of the login methods enabled by Novell and third-party authentication modules.

For this example, suppose that the Tai-Hao smart card method is method 25 and the Precise Biometrics’ fingerprint method is method 26. Patrick’s workstation client has methods 25 and 26 installed, and Patrick is attempting to use both. The message from the NMAS client indicates that Patrick’s workstation client can do methods 25 and 26. Suppose, for this example, that this message also indicates that the login sequence Patrick requested requires method 25 to be completed first, followed by method 26.

When the NMAS server is thus satisfied, it returns a message to the NMAS client indicating that this portion of the login sequence is done and successful. Both the LSM and LCM then return to NMAS.

The NMAS client stores these credentials in a secret storage, and when Patrick attempts to access information, the server on which that information is stored asks Patrick’s client for Patrick’s eDirectory credentials. As requested, the NMAS client returns information about the Tai-Hao smart card method. During this process, the LCM invokes the method-specific user interface that requests the necessary login factors.

What does this mean? Users who want to access volumes graded at the Password&Token level must have Password&Token security clearance. These users also have the right to log in to the network using the network’s password and token method—in this case, the Tai-Hao smart card method. Similarly, if users want to access volumes graded at the Biometric&Password&Token level, they need equivalent security clearance. They also need access to the network using the network’s password, token, and biometric method—in this case, the Precise Biometrics fingerprint method.

**NMAS in Action**

For example, suppose that Patrick in Accounting is logging in to the network for the first time, or suppose that he is requesting Password&Token clearance for the first time. On the initial login screen, Patrick enters his eDirectory username and then clicks the Advanced button. (See Figure 3 on p. 27.)

When Patrick clicks the Advanced button, two additional fields appear under the NMAS tab: Sequence and Clearance. Patrick enters the name of the login sequence he will use in the Sequence field—in this case, Payroll. Patrick then enters the clearance level he is requesting in the Clearance field—in this case, Password&Token. Both of these fields also have Browse buttons that enable users to choose from a list of available login sequences or clearance levels.
Patrick then responds to prompts by entering his password and swiping his smart card. When he clicks OK—assuming he has entered the correct information and that the MIS specialists have assigned him the clearance he has requested—he is authenticated to eDirectory. Patrick then gains access to the volume and partition that hold the payroll data (assuming his ACLs also grant him access to this level of access).

Patrick completes these fields only the first time he logs in or each time he requests a login sequence and clearance level that differs from the login sequence and clearance level he last requested. Otherwise, Patrick enters only his username and Enter, after which the login sequence and clearance level he last entered are invoked. (For more information about what goes on behind the scenes during this login process, see “NMAS Under Cover.”)

Enable Remote Access

Few users have access to the Taipei County Government network from outside its firewall, and employees must request special permission to gain access. At this point, approximately 100 employees have requested and received permission to access the network from outside the firewall.

To enable Taipei County Government’s remote and mobile employees to access the network from outside the firewall, UniBiz installed a Cisco 2500 Series Access Server (www.cisco.com/univercd/cc/td/doc/pct/2500as.htm). The Cisco Access Server communicates with the BMAS 3.6 server that UniBiz installed on the NetWare 5.1 server that is running the eDirectory objects.

Both the Cisco Access Server and BMAS 3.6 support the Remote Access Dial-In User Service (RA DIUS) protocol. (You can read about the RA DIUS protocol in RFC 2138 and 2139. You can download these RFCs at www.ietf.org/rfc/rfc2138 and www.ietf.org/rfc/rfc2139, respectively.) Incidentally, the RA DIUS services offered by BMAS are now available in NMAS 2.0.

To gain access to Taipei County Government’s network, remote and mobile employees dial a local number to access the Cisco server. When prompted, these employees then enter their eDirectory username and password. This server uses RA DIUS to pass this authentication information to the BMAS server. BMAS removes the eDirectory username and password from the RA DIUS package and uses Novell Core Protocol (NCP) to pass this authentication information to eDirectory (running on the same server).

eDirectory then checks the received username and password against the user name and password it has stored for each particular employee. If the information matches, eDirectory uses NCP to return to BMAS the decision to grant this employee access. BMAS then uses RA DIUS to forward this decision to the access server.

Both the Cisco Access Server (as with any access server) and the BMAS RA DIUS server (that is, the RA DIUS, NLM running on the BMAS 2.6 server) are eDirectory clients. Thus, Taipei County Government’s MIS specialists can manage both servers and can control users’ access to those servers just as they manage and control access to other eDirectory objects.

WHAT’S DONE AND WHAT’S NEXT?

The Novell access and security solution is the solution that Taipei County Government was looking for. Because this solution has eDirectory at its core, the organization now has a central location for storing identity information, authentication credentials, and access control policies. With eDirectory and Novell Access Management 2.1, Taipei County Government now enjoys the effects of consolidated user accounts: Employees need enter only one set of credentials to access all of the network resources to which they have rights; MIS specialists manage access rights from a central location—including access rights for the 100 remote users who access the network via BMAS 3.6.

Most important in the context of this security-focused issue of Novell Connection, this solution better protects the organization’s information systems. For one thing, because employees have only one set of credentials to memorize, they are less likely to write down these credentials and are thus less likely to compromise security. For another thing, MIS specialists now confidently assign from a central location the access rights employees need. Equally confidently, MIS specialists delete or disable access rights as needed.

Of course, Taipei County Government has increased security through its use of multifactor authentication methods enabled through NMAS 1.0. The organization no longer protects its most important and confidential resources with only passwords, which take no more than a good guess to break. Instead, Taipei County Government protects such resources with combined login factors.

To access these protected resources, employees with the necessary rights must enter an eDirectory password and a smart card. For some highly confidential resources, employees with rights must provide an eDirectory password, smart card, and fingerprint to gain access.

Taipei County Government has come a long way but still has a bit further to go to complete its planned access management project. For example, Taipei County Government plans to upgrade to Microsoft Exchange 2000, for which it will install a new Windows 2000 server running Microsoft Active Directory. Naturally, the organization will integrate the resulting new accounts with eDirectory.

Taipei County Government also plans to upgrade to NMAS 2.0 and is considering deploying Novell SecureLogin, which enables true single sign-on. With Novell SecureLogin, Taipei County Government could optimize security by assigning employees separate passwords or other login factors to access various applications. However, the employees wouldn’t need to even know about these separate credentials. Novell SecureLogin would handle the process of signing on to these applications behind the scenes. Employees would enter their eDirectory credentials (which may include a password, a smart card, a fingerprint, or any combination of the three) only once. Ever after, when employees attempt to access applications that require additional credentials, Novell SecureLogin would sign on to these applications on the employees’ behalf.

Regardless of its future plans, Taipei County Government’s new approach to its old problem is already serving its purpose. Employees now enjoy managing only a single set of credentials to access all network resources. MIS specialists now save a considerable amount of time by having only one user account to manage per employee. Finally, and arguably most important, Taipei County Government now knows it has taken at least preliminary steps to better protect and secure its information systems.

Linda Kennard works for Niche Associates, a technical writing and editing agency located in Sandy, Utah.