

strengthening airport and airline security

Industry Vertical

www.novell.com

WHITE PAPER

N

Novell.

table of contents

strengthening airport
and airline security

2	IDENTIFY, ASSESS, DISSEMINATE AND ACT
2	EXECUTIVE SUMMARY
3	ENSURING AIRPORT SECURITY— A DAUNTING CHALLENGE
6	IDENTITY MANAGEMENT—LAYING THE FOUNDATION FOR STRONG AIRPORT AND AIRLINE SECURITY
7	REQUIREMENTS FOR AN EFFECTIVE MANAGEMENT INFRASTRUCTURE
11	THE NOVELL IDENTITY MANAGEMENT INFRASTRUCTURE
13	CONCLUSION
14	LINKS TO ADDITIONAL INFORMATION
14	NOVELL IDENTITY MANAGEMENT INFRASTRUCTURE PRODUCTS & RELATED ALLIANCE/INDUSTRY PARTNER PRODUCTS & SOLUTIONS

identify, assess, dissemiNate and act

Making the skies safer for passengers remains a top priority as the air transportation industry struggles to recover in the aftermath of the September 11, 2001 terrorist attacks. The Security Act of 2001 signed by U.S. President George W. Bush in November set forth a number of new and enhanced security measures aimed at preventing future terrorist acts.

The measures call for airlines to install stronger doors to prevent terrorists from getting into cockpits, and mandate the placement of armed air marshals on many commercial flights. Flight crews are now being instructed to resist hijackers rather than give in to their demands. There are tighter restrictions on what items are permitted in carry-on bags. All checked baggage is screened for explosives or matched to passengers. And later this year, federal employees will assume responsibility for security at many U.S. airports.

Perhaps the greatest challenge facing those responsible for airport security and airline safety is the ability to identify, assess, disseminate and when necessary, act on passenger and employee information quickly and effectively. This information must consolidate data from a variety of sources, such as immigration, passport, customs and travel visa administration databases and law enforcement watch lists.

EXECUTIVE SUMMARY

Technologies are now available that can help meet the challenge of airport security and airline safety. These technologies substantially improve the ability of airports and airlines to quickly and accurately identify terrorists, criminals and other individuals who might pose an immediate threat to security and safety. Moreover, these technologies can enable tight control of access to sensitive areas—airplanes, flight operations facilitates, baggage-handling areas and even travel reservation systems.

These new technologies include biometric devices such as facial recognition or fingerprint identification systems, hand-recognition scanners, and iris or retinal scanners to identify individuals uniquely. When used alone or in conjunction with other security mechanisms such as passwords, digital certificates and smart cards, biometric technology greatly reduces the chances of individuals gaining access to restricted areas in airports or hacking into air transportation computer systems.

The foundation for this enormous security effort is an infrastructure that enables the management of digital identities. These identities include comprehensive information, such as an individual's authentication information, relationship and role, and personal data. Identity information can facilitate faster, more active sharing of critical security information between the airlines, airport authorities, law enforcement, the newly created Transportation Security Administration and other government agencies.

This paper describes the importance of identity management in bolstering airport security, making air travel safer and streamlining the flow of low-risk passengers at airports. It examines the requirements that an identity management infrastructure must meet to be effective. It also presents the Novell® identity management infrastructure—a scalable, reliable, secure infrastructure that enables airports and airlines to address the challenges they face in implementing short- and long-term solutions for strengthening airport security and ensuring aircraft and passenger safety.

ENSURING AIRPORT SECURITY— A DAUNTING CHALLENGE

The terrorist attacks on the World Trade Center and the Pentagon brought to the forefront the urgent need to improve airport security and to safeguard commercial airline travel. The magnitude of the attacks brought intense pressure from the public to identify shortcomings in aviation security policies and to “do whatever it takes” to reduce or eliminate the risk of such attacks happening again.

In response, governments and regulatory entities around the world are creating new airport security agencies, allocating funds for technology and passing legislation mandating additional and more stringent airport security measures. The Canadian government allocated Canadian \$2.2 billion for a broad range of initiatives designed to enhance and improve security operations at airports and help minimize the threat of terrorist attacks. In the U.S., President Bush is seeking to spend US\$52 billion for federal information technology (IT) programs in fiscal 2003—“a dramatic 15.6 percent increase stemming from the administration's focus on using IT to improve government performance and the response to the September 11 terrorist attacks.” Bush's proposed budget also devotes US\$38 billion to homeland security, including US\$722 million for using IT to improve information sharing.

To ensure the ongoing security and safety of airports and passengers, it's imperative that airport authorities, airlines and related organizations address two critical issues:

- Controlling employee access to airport facilities, including the nonobtrusive monitoring of employee activities.
- Reducing the turmoil and decreasing the wait time for passengers at check-in and at all processing checkpoints, while at the same time increasing the overall level of security.

Controlling Employee Access to Airport Facilities

Airport authorities, airlines, government agencies and law enforcement agencies face many of the

According to Senator Jay Rockefeller (D-W. Va.), chairman of the Senate Commerce, Science and Transportation Committee's Aviation Subcommittee, technology is more important than ever to airport security. “We must be able to monitor and share real-time information about who is getting on a plane, what are they bringing with them, who has access to airport security areas and aircraft, and ultimately, whether all of those people really are who they claim to be.”

same challenges that other organizations must contend with in controlling access to facilities. These challenges include the large and growing number of people who need access, as well as the realization that simple password mechanisms are inadequate for ensuring access control. Because people rarely update passwords or are careless about keeping them private, passwords are common targets of theft. This significantly increases the opportunities for unauthorized people to gain entry into sensitive areas of the airport.

In addition, the disparate, isolated systems used for tracking employee information are often difficult to manage and maintain, and quite frequently result in serious security loopholes. Revoking an employee's access privileges usually means manually removing that individual from several systems. All too often, terminated employees are not removed from all applications and security systems. In both Canada and the U.S., there is concern that at some airports hundreds or possibly thousands of security badges are unaccounted for.

This type of situation seriously compromises airport security and passenger safety. Former employees could easily gain access to restricted or controlled areas of the airport. Even worse, criminals and terrorists could obtain lost or stolen passes illegally and use them to enter restricted areas in airports or to board aircraft.

And the problems don't end there. Current systems don't easily support graded levels of authentication that allow employees to move freely within areas they are authorized to enter,

and at the same time, prevent them from entering areas that are restricted or off limits. Some employees need wider access to airport facilities due to their jobs. As a result, they require a higher-level screening. For example, background checks for people who will work in highly sensitive locations in the airport—such as aircraft maintenance or flight operations facilities—must be more in-depth than those for people in food or custodial services. Without graded authentication, employees who haven't been carefully screened could potentially gain access to highly restricted areas and do so without detection.

Further complicating the problem is the fact that current systems don't provide a thorough audit trail of each employee's movements in and out of restricted areas. Nor is there any mechanism for alerting the appropriate people when an unauthorized individual enters a restricted area or when an employee's movements seem excessive or in some other way suspicious.

Airport authorities and airlines can ensure that only authorized staff can gain entry to specific areas by implementing biometric identity solutions that use data such as face recognition, fingerprints, iris scans or other forms of biometric information to identify employees. Biometric information can be combined with other employee information and stored in an identity management directory, then duplicated on a smart card that serves as the employee's ID card. The identity management directory also defines the employee's access to physical locations and information network resources, such as passenger reservation systems, within the airport.

According to *InformationWeek*, the U.S. Federal Aviation Administration (FAA) is already in the process of developing standards and mandates for airport security using smart-card, public key infrastructure (PKI) and biometric technologies. Initially, the agency wants to create a smart card for all airline, airport and FAA employees to control access in airports. The employee's photo and personal demographic data would be added to the card along with some type of biometric data. Eventually, the technology could be used to accommodate travelers as well.

A solution that includes biometric identification provides strong protection against unauthorized people who attempt to use a lost or stolen ID card to access restricted areas or computer systems. It also increases accountability for employees' time and whereabouts. Support for multiple forms of authentication—for example, smart card, hand geometry and fingerprints—is important because it enables organizations to evolve the solution to incorporate additional identification methods without ripping and replacing the entire system.

Reducing Turmoil and Decreasing Wait Times for Passengers

Security is being tightened dramatically at airports around the world. Many of the conveniences once enjoyed by travelers have been eliminated. In some airports, curbside check-in and parking in or near terminals is restricted. Only ticketed passengers are allowed beyond security checkpoints. More in-depth screening procedures, including frequent hand-wand checks, pat downs and searches of carry-on bags are now commonplace. In some places, passengers

are required to present government-issued ID to board planes.

These increased restrictions are necessary to ensure security. Unfortunately, current systems are ill equipped to handle the increased demands of newly implemented security measures. As a result, security procedures at many airports are creating lengthy delays for passengers and generating chaos and additional costs for airlines and airports.

Security screeners, for example, are at risk of becoming fatigued and stressed, which can lead to serious security risks. By reducing the need for humans to visually scan bags security can be increased and passengers can move through the airport more quickly.

The added security procedures are also taking a toll on travelers. Passenger anxiety and stress levels often result in desperate or disruptive behavior such as trying to bypass the system to avoid missing a flight. For example, a passenger traveling through Atlanta's Hartsfield International Airport ran through a security checkpoint to retrieve his camera and get back to the gate to catch his flight. As a result of the security breach, the airport was shut down, causing a major disruption in service.

To alleviate much of the turmoil and the long waits associated with check-in and security procedures, airport authorities and airlines could create automated check-in and security inspection kiosks for frequent fliers and other passengers who are willing to provide identity information in advance. This type of system could leverage

"No matter how well trained or well paid you are, if you are sitting at a scanning station for more than an hour at a time, you are probably going to drift off occasionally. But if there is a way to automate the whole process, with fingerprint recognition techniques or highly sophisticated scanners, we'd be a lot better off."

—Richard Gritta
Airline Industry Expert
University of Portland

In a November 2001 survey by eMarketer, Inc., 16 percent of business travelers and 14 percent of leisure travelers reported they were canceling or taking fewer trips after September 11 because “air travel has become too big of a hassle.”

identity programs such as driver’s licenses, passports, national identity cards, frequent flier ID cards or specially issued smart cards. In addition, the system would include biometric information for positive identification.

At check-in time, enrolled passengers could present their passenger identity card, which would be compared against the pre-stored data. Any discrepancies could be reported to an inspector for immediate investigation. Likewise, these passengers could run the identity card through a security inspection kiosk and provide biometric information, which the security system would use to validate the identity, check security databases and determine whether or not to allow the passenger to proceed.

Solutions that make use of “fast track” check-in and security screening would facilitate and speed the movement of passengers without jeopardizing security. They would also reduce the workload and pressure of overburdened security staff, lessen the risk of human error, and decrease the number of people in traditional passenger screening checkpoints, thereby expediting those inspections as well.

IDENTITY MANAGEMENT—LAYING THE FOUNDATION FOR STRONG AIRPORT AND AIRLINE SECURITY

In designing new systems, a distinction must be made between security processes aimed at airport and airline personnel, and those designed to handle passengers. The key to addressing the specific requirements for both groups is a comprehensive identity management infrastruc-

ture that maintains a unique identity for each employee and traveler.

Digital identities can contain a variety of information:

- **Authentication information** typically includes name, password, digital certificates and biometric data.
- **Relationship information** defines relationships and roles. For employees, it would specify whether or not the employee has access to restricted areas as well as when, how often and under what circumstances the employee could enter those areas. For passengers, this information would indicate if the person is enrolled in an express check-in and security inspection system.
- **Personal information** includes telephone numbers, email and postal addresses, and driver’s license, passport, national identity card or social security numbers. It also includes biometric information.

The identity management infrastructure provides the foundation for two important system services: security and activity tracking.

Security

The security service provides three essential functions:

- **Authentication** ensures that the employee or traveler is who he or she claims to be. This is essential for preventing people from masquerading as others to gain entry into restricted areas of the airport or board an aircraft.

- **Authorization** determines which physical facilities an employee or passenger is authorized to enter. It is typically based on the individual's relationship and role. In the case of an employee, access is based on job requirements. For example, access for pilots and aircraft maintenance personnel differs significantly from that of food service and custodial employees.
- **Access control**, also based on relationship and role, ensures that people have access to everything they are authorized to use and denies access to all other resources. Access control also limits the level of access privileges. Control could make use of smart cards, hand-recognition scanners and other devices to limit entry to specific areas of the airport.

Activity Tracking

Tracking services provide accountability, nonrepudiation and auditing of all critical activities in an airport.

- **Accountability** involves tying a tracked activity to a specific person—for example, an employee entering a restricted area or a passenger going through a security checkpoint.
- **Nonrepudiation** proves undeniably that a particular person entered a specific area or performed a particular tracked activity.
- **Auditing** involves maintaining a complete trail of all tracked activities, such as monitoring a passenger's journey from check-in to the boarding gate or following the activities of a baggage handler while on the job. These three

activity-tracking services are essential to ensuring airport security and passenger safety.

REQUIREMENTS FOR AN EFFECTIVE IDENTITY MANAGEMENT INFRASTRUCTURE

An identity management infrastructure must meet several important requirements to be effective.

This section examines those requirements and provides air transportation industry professionals with criteria for selecting an infrastructure that will enable them to:

- Exchange identity information across organizations and agencies in real time.
- Continuously improve the efficiency and effectiveness of security processes and procedures.
- Streamline the flow of passengers and visitors through the airport.

Single Point of Management

In the air transportation industry, identity information is spread across multiple systems in multiple organizations. Airlines maintain employee and passenger data. Airports maintain employee data. Concessionaires, such as stores and food service areas, maintain employee data. Government agencies maintain data on federal employees working at airports as well as passport control data and law enforcement watch lists.

The situation is further complicated by the fact that each organization has a separate system for tracking identities. As a rule, these systems don't integrate readily with each other, so the organizations involved cannot easily share identity

information and cooperate effectively. Consequently, law enforcement agencies may not know when individuals on watch lists or with criminal histories are hired, or when passengers on watch lists enter the country. And employers may not know when they have hired people who are on watch lists or who have criminal histories.

In an effort to identify high-risk travelers for bag searches or interviews, both the U.S. and Canadian governments recently established a requirement that airlines provide passenger lists to arriving airport security personnel two hours before a flight lands in the U.S. or Canada. According to *Government Computer News*, President Bush wants to use technology to track the arrivals and departures of all visitors to the United States. This objective necessitates tight integration across identity management systems to be effective.

Moreover, IT administrators within each organization typically enter identity information manually into multiple systems—human resources, security and IT networks. This costly and error-prone process could—and often does—result in security lapses.

An identity management infrastructure should provide a single point of management for all identities. Administrators enter identity information once in a single database that is then automatically distributed to all data stores. This automation saves the administrator considerable time, ensures accuracy and eliminates security holes.

Single-point management also enhances security by enabling immediate revocation of all

access rights when an employee is terminated or a passenger is flagged as high risk. The employee or passenger is immediately prohibited from entering restricted or controlled areas or from boarding aircraft.

Permit Management Delegation

The identity management infrastructure should allow delegation of management. In this way, each airline, airport authority, government or law enforcement agency can maintain its autonomy. Delegation also moves the administration of identities into the hands of the people who are closest to employees and passengers.

Support Identity Information Sharing

It's critical that an identity management system support inter-agency sharing of employee and passenger information. This requires that the infrastructure support integration across disparate systems in diverse organizations. Integration permits information sharing that enables government and law enforcement agencies, airlines and airport authorities to identify employees with criminal records, or flag employees or passengers who are on terrorist or criminal watch lists.

Support Strong Multilevel Security

The system should support graded levels of security that permit the implementation of stronger security mechanisms for more sensitive areas. For example, stronger security should be implemented for entry into an aircraft maintenance area than for entry into a janitorial supplies closet. Graded security requires that the identity

Scenario example:

An example of how this works is to take a hypothetical passenger named Bob. Bob has traveled a few times in the past year so his generic profile, or “identity,” is stored in the airline database. As Bob approaches the ticket counter, he is able to identify who he is by either handing over a smart card to the ticketing agent or using his thumbprint to authenticate who he is to the system. As far as the airlines’ database is concerned, Bob is a model citizen and everything is in order.

However, in a different database kept at a law enforcement headquarters in Washington, D.C., information is being kept on Bob as a possible terrorist suspect. Because the airlines’ database is not integrated with the terrorist database kept at the law enforcement agency, the airport is unaware of the potential risk and threat Bob presents. With Novell technologies helping to integrate these two disparate databases, a situation where a possible terrorist goes unidentified wouldn’t have happened.

Novell technologies in concert with technologies provided by our solution partners, will allow the airline and law enforcement agencies to share specific data about an individual automatically and securely according to the business policies and agreements made between the two organizations; therefore, only the information about Bob that needs to be shared is shared.

Following deployment of Novell’s identity management technologies, whenever Bob approaches the ticket agency and “identifies” or authenticates himself to the system, the ticket agency will be informed about the potential risk and can deal with it according to the airline’s policies.

In addition to providing a solution for improving the quality of data about passengers like Bob, organizations can also use these same technologies to immediately synchronize updated information and access rights for any identity. Whether it be an airport employee or passenger, all access rights to the network are instantly revoked and areas requiring authentication are immediately disabled; furthermore, a new law enforcement officer entering into a scene can be instantly granted access to all needed information and assigned access to the areas he needs to be.

management system support multilevel security mechanisms, such as password, smart card, digital certificates and biometric devices.

Prevent Unauthorized Access to Identity Information

Because identity determines access rights, identity information must be protected with the strongest security possible. Only trusted,

authorized people, such as system administrators, should be able to access and change it.

This high level of security requires strong authentication mechanisms such as those provided by digital certificate, smart card, token and biometric technologies. Strong security prevents unauthorized people—employees, passengers, visitors, criminals or would-be terrorists—from accessing and changing identity information.

Leverage Existing Systems and Technologies

Most entities involved in air travel have invested a substantial amount of money in IT systems and infrastructures. Few, if any, can afford to throw out their current systems and implement completely new ones. In addition, recent government mandates have set deadlines for the implementation of new security policies and procedures, so delays are unacceptable. Therefore, it's essential that the identity management infrastructure leverage existing systems and technologies wherever possible instead of requiring organizations to rip and replace.

Many organizations already have huge volumes of identity information stored in human resources applications, travel reservation systems and other applications and databases. Reentering or relocating this data may be impractical or economically unfeasible. Consequently, the infrastructure must be capable of accessing, using, and automatically updating data between all databases. Furthermore, database owners closest to sensitive information must maintain authoritative control over updating and sharing their data—wherever they sit on the network.

Finally, the identity management infrastructure should be capable of leveraging existing security mechanisms that run on popular operating platforms. It should also support industry standards to keep options open and ensure that airports, airlines, government agencies, law enforcement and others aren't locked into a single-vendor environment that limits their ability to adapt, evolve and grow their systems.

High Availability and Fast Performance

Airports operate 24x7x365, so identity information must be available at all times and access must be virtually instantaneous. That means the identity management infrastructure must be resilient to hardware failures and other system problems. It must also be highly efficient to ensure fast performance so that passengers don't encounter significant delays during the check-in, screening or boarding processes, and employees have timely access to authorized locations in the airport.

One way to achieve around the clock availability of identity information is to replicate and synchronize it across multiple servers on the network. If one server isn't available—whether due to a failure or routine maintenance—the identity information is still available from another server. Replication has the added benefit of boosting performance by bringing identity information closer to the point of access. Another way to ensure continuous availability is to allow administrators to modify identity information without shutting down the system.

Extensive Scalability

Airline travel involves huge numbers of participants. The volume continues to grow and could easily approach tens of millions. Therefore, the identity management infrastructure must offer extensive scalability so it can support an ever-increasing number of identities. Organizations should be able to scale the system by adding servers as well as by adding processors to existing servers. Administrators should be able to add capacity without shutting

down the system, ensuring that crucial identity information is always available.

THE NOVELL IDENTITY MANAGEMENT INFRASTRUCTURE

Novell's identity management infrastructure meets, and even exceeds, the requirements for an effective identity management solution for ensuring airport security. The infrastructure is supported by a broad range of Net services software from Novell and its partners (see Figure 1). Because of its directory foundation and modular design, the Novell identity management infrastructure provides a scalable, reliable and secure foundation for controlling employee access to facilities as well as streamlining passenger security inspections, while making them more secure.

Simplifies Identity Management

The Novell infrastructure provides IT managers with a single point of management. Single-point management greatly simplifies the administration of employee and passenger identities, and also enables effortless yet secure sharing of information

across various organizations. Because the Novell infrastructure permits delegation of identity management, it preserves organizational autonomies and puts administrative responsibilities in the hands of those closest to employees and passengers.

The administrator simply drags and drops individuals into the appropriate place in the directory based on business relationship and role. The administrator can easily move people within the directory, automatically changing access profiles as relationships or roles change. In addition, removing an identity from a single location, Novell eDirectory™, terminates all access privileges immediately for that person. This allows the administrator to revoke access instantly for people who are no longer employed by the airport or airline—bolstering security by reducing the risk of unauthorized entry into restricted areas.

Secures Identity Information

The Novell infrastructure protects the management of identities with strong security options that meet even the most demanding security standards. Individuals must be authenticated to Novell eDirectory to gain access and the infrastructure

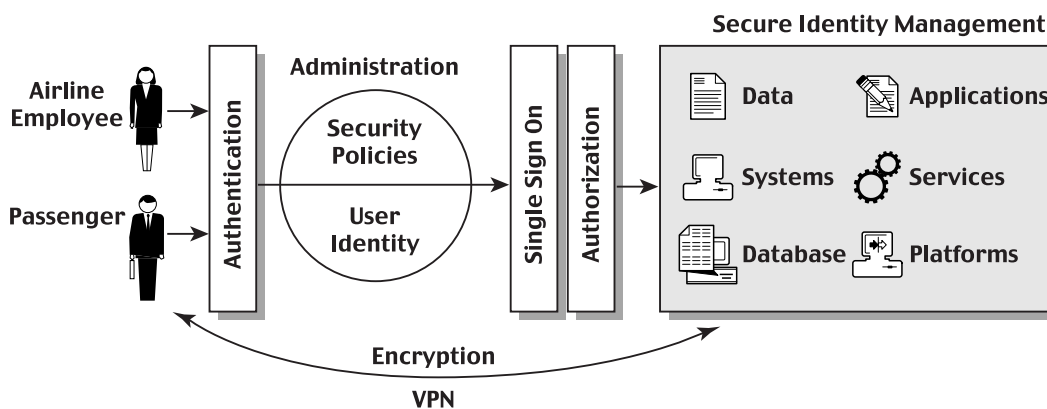


Figure 1. The Novell Identity Management Infrastructure.

“Since 9-11 there’s a large interest in redundant networks, network diversity—that is, more than one provider—increased security and managed services. It’s no longer business as usual on the government side.”

—John Polivka,
Sprint spokesman

supports multilevel authentication including passwords, smart cards, tokens and biometric devices. Moreover, all sensitive identity information in the directory is encrypted to prevent theft. The infrastructure encrypts all sensitive identity information sent over the wire using industry-standard encryption mechanisms, making it unreadable by hackers and eavesdroppers.

The Novell infrastructure also tracks all critical activities performed on the directory, such as adding, deleting or changing identity information. This tracking permits full accountability, reliable nonrepudiation and extensive auditing of directory activities to ensure the integrity, confidentiality and availability of identity information.

Leverages Existing Investments

The Novell identity management infrastructure fits easily into existing network environments because it runs on multiple platforms and supports all popular industry standards. As a result, air travel industry organizations can preserve their significant investments in systems and technologies. The infrastructure runs on NetWare®, Windows NT®, Windows® 2000, Tru64®, Solaris® Sparc®, AIX® and Linux®. It supports important directory standards, such as Extended Markup Language (XML) and Lightweight Directory Access Protocol (LDAP). Through LDAP, the infrastructure can communicate with other LDAP-compliant network directories, enabling organizations to leverage the identity information already stored in existing directories.

In addition, the infrastructure can use Novell DirXML® technology to access identity information

stored in other data sources, such as applications and databases. With DirXML, data owners can designate any directory or database as the authoritative source of information, as well as define business rules that govern what happens when data modifications take place and how those modifications will be reflected in or replicated to other information systems.

Organizations can leverage any security mechanisms they have in place, such as Resource Access Control Facility (RACF®), Windows NT and UNIX® security systems. Most importantly, the infrastructure ties all these systems back to a single identity maintained in Novell eDirectory, dramatically simplifying security management and system use.

The infrastructure can transparently PKI-enable existing Web, Windows and legacy applications for digital certificate authentication without having to modify the applications. It can also validate any vendor’s x.509 v3-compliant certificate during authentication process.

The open standards approach of the Novell infrastructure eliminates the risks associated with locking into a single vendor. These risks include lack of flexibility, higher cost and slower access to new technologies.

Ensures High Reliability and Availability

Novell eDirectory has been field proven in nearly 10 years of use by thousands of organizations and more than 230 million users worldwide. It has consistently demonstrated high reliability and stability, and the ability to perform in large,

complex enterprise environments. The infrastructure can automatically replicate Novell's eDirectory across the network to ensure its availability in the event of server failure, so that critical information and resources are readily accessible at all times.

Scales to Meet Expanding Needs

The Novell identity management infrastructure is the only one that scales to Internet proportions. Novell eDirectory has been tested with over one billion objects. In contrast, Microsoft* Active Directory* uses the JET database (Microsoft Access*) and users are cautioned against putting more than 5,000 users in a single database.

Novell eDirectory fully exploits the power of multiprocessor servers and it permits the addition of servers without shutting down the system. As a result, organizations can easily expand their systems to support a growing user base and increasing demands for services—*without service disruption*.

Provides Authentication and Access Control Services

Novell and its partners provide a variety of services built on the infrastructure to facilitate authentication, authorization and access control. These services support graded access control with multilevel authentication, including passwords, x.509-compliant smart cards, tokens such as RSA* and Vasco*, and biometric devices. As a result, organizations can choose the appropriate security mechanisms based on specific needs and circumstances. They also have the flexibility to add security mechanisms as their needs evolve, without ripping and replacing the overall system.

Access control services give employees and passengers immediate access to all the facilities they are permitted to enter but restrict entry into other areas. These services readily interface with various third-party card and biometric systems to provide complete access control solutions.

CONCLUSION

Since September 11, the air transportation industry has been under enormous pressure to implement a broad range of new airport security measures in response to the ongoing threat of terrorism. At the same time, for the industry to remain viable and recover, it must convince potential travelers concerned about security and long delays at airports that flying is still a safe and convenient method of transportation. The industry is looking to information technology for help in addressing these challenges.

Fortunately, many powerful technologies are available to help the air transportation industry implement systems that significantly improve security at airports and keep passengers moving through the system efficiently. An identity management infrastructure is the foundation of such a system. That's why it's essential to select an identity management infrastructure that offers the availability, performance, scalability, security, flexibility and ease of management that the air transportation industry needs to deal with internal and external security issues and help them to regain public trust and confidence in the system.

Novell and its partners offer an identity management infrastructure that meets all of these requirements and can also help airports and airlines

simplify, secure, accelerate and extend their compliance with current and pending aviation security legislation. Because many airlines and airports already have the Novell infrastructure in place, they can quickly and cost effectively leverage their technology investments by integrating and deploying new systems for screening passengers and employees.

Finally, the Novell identity management infrastructure positions the air transportation industry to team up with government agencies and law enforcement to proactively address security and safety issues by developing systems that allow them to take preemptive action by identifying potential terrorists or suspicious behaviors before there's a problem.

LINKS TO ADDITIONAL INFORMATION

Novell, Inc.	http://www.novell.com
Novell Customer Success Stories	http://www.novell.com/success/by_industry.html#government http://www.novell.com/success/by_industry.html#transportation http://www.novell.com/success/by_industry.html#other
Novell Net Services Software Helps Airlines Take Flight and Airports Stay Grounded (Press Release)	http://www.novell.com/news/press/archive/2001/06/pr01061.html
Lufthansa Takes on Metadirectory Solutions from Novell (Press Release)	http://www.novell.com/news/press/archive/2002/01/pr02009.html

NOVELL IDENTITY MANAGEMENT INFRASTRUCTURE PRODUCTS & RELATED ALLIANCE/INDUSTRY PARTNER PRODUCTS & SOLUTIONS

Novell eDirectory	http://www.novell.com/products/edirectory
Novell DirXML	http://www.novell.com/products/edirectory/dirxml
Novell Modular Authentication Service	http://www.novell.com/products/nmas
Novell ZENworks®	http://www.novell.com/products/zenworks
Novell SecureLogin	http://www.novell.com/products
/securelogin	
Novell iChain®	http://www.novell.com/products/ichain
Deloitte & Touche (Alliance partner)	http://www.us.deloitte.com
RSA Security (Industry partner)	http://www.rsasecurity.com
VASCO (Industry partner)	http://www.vasco.com
SecuGen Corporation (Industry partner)	http://www.secugen.com
Activcard® (Industry partner)	www.activecard.com
Arcot Systems, Inc. (Industry partner)	www.arcot.com/products/nmas.html
BioID® (Industry partner)	www.bioid.com
Biometricate (Industry partner)	www.biometricate.net
Biometric Access Corporation (Industry partner)	www.biometricaccess.com
Cherry Corporation (Industry partner)	www.cherrycorp.com
Compaq (Industry partner)	www.compaq.com/products/options/fit/index.html
Identix (Industry partner)	www.identix.com
SafLink (Industry partner)	www.saflink.com
Secure Computing (Industry partner)	www.securecomputing.com
Veridicom Inc. (Industry partner)	www.veridicom.com
VisionSphere Technologies (Industry partner)	www.visionspheretech.com/its_me-novell.htm

© 2002 Novell, Inc. All rights reserved. Novell, NetWare, DirXML, iChain and ZENworks are registered trademarks, and eDirectory is a trademark of Novell, Inc. in the United States and other countries.

*Active Directory, Microsoft, Microsoft Access, Windows and Windows NT are registered trademarks of Microsoft Corporation. Tru64 is a trademark of Compaq Computer Corporation. UNIX is a registered trademark of X/Open, Ltd. Solaris and Sparc are registered trademarks of Sun Microsystems, Inc. Microsystems, Inc. AIX and RACF are registered trademarks of International Business Machines Corporation. Linux is a registered trademark of Linus Torvalds. RSA is a trademark of RSA Data Security, Inc. Vasco is a registered trademark of VASCO. All other third-party trademarks are the property of their respective owners.

Novell Product Training and Support Services

For more information about Novell's worldwide product training, certification programs, consulting and technical support services, please visit:

www.novell.com/services

For More Information

Contact your local Novell Authorized Reseller, or visit the Novell Web site at: www.novell.com

You may also call Novell at:

1 888 321 4272 US/Canada
1 801 861 4272 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.

1800 South Novell Place
Provo, Utah 84606 USA

www.novell.com

Novell