

**The Identity Infrastructure:
Security Starts With The Right Foundation**

W H I T E P A P E R

Copyright © 2002 Oblix, Inc. All rights reserved.

This white paper is for informational purposes only. Oblix makes no warranties, expressed or implied, in this document. Mention of third-party products within this publication is for informational purposes only and constitutes neither an endorsement nor a recommendation.

The information contained in this document represents the current view of Oblix on the issues discussed as of the date of the publication. Because Oblix must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Oblix, and Oblix cannot guarantee the accuracy of any information presented after the date of publication.

Software and documentation Copyright © 1996-2002 by Oblix, Inc. All rights reserved. Oblix, NetPoint, Oblix NetPoint, Oblix NetPoint 6, NetPoint COREid System: User Manager, Group Manager, Organization Manager, IdentityXML, Certificate Processing Server (VeriSign®), COREid Server, and WebPass; NetPoint Access System: Access Manager, Access Server, WebGate, and AccessGate; COREid, FEDERATEDid Layer, Oblix IDLink, Associate Portal Services, NetPoint System Console, NetPoint Ready Realm, NetPoint Federation Services, NetPoint Mainframe Security Connector, and their logos are trademarks of Oblix, Inc. All other company and product names are trade names, service marks, trademarks or registered trademarks of their respective companies.

Printed in the United States of America.

Printing Date: October 2002

Part Number: obx10b

Oblix, Inc.
18922 Forge Drive
Cupertino, CA 95014, USA
Tel: 408.861.6800
Fax: 408.861.6810

European Headquarters
Atrium Court
The Ring, Bracknell
Berkshire, RG12 1BW, UK
Tel: +44 (0)1344 393054
Fax: +44 (0)1344 393154

www.oblix.com
info@oblix.com

| | |
|--|-----------|
| Creating Collaborative Environments | 1 |
| Securing Shared Resources | 1 |
| Oblix NetPoint: The Foundation of an E-Business Network | 2 |
| E-business Network Challenges | 3 |
| Managing Complex User Environments | 3 |
| Creating Individualized Access Control | 4 |
| Serving Organizations in Continuous Motion | 5 |
| Infrastructure Essentials | 6 |
| Access Control | 7 |
| Enterprise Identity Management (EIM) | 8 |
| Scalable Administration | 10 |
| Oblix NetPoint: A Complete Identity Infrastructure | 11 |
| COREid | 11 |
| Delegated Administration | 11 |
| Identity Workflow | 12 |
| Group Management | 13 |
| IdentityXML | 13 |
| FEDERATEDid Layer | 13 |
| Web Access Management | 14 |
| Integration with Web Infrastructure Applications | 15 |
| Provisioning | 15 |
| Integration Services | 15 |
| Conclusion | 16 |
| References | 17 |

Creating Collaborative Environments

In today's increasingly competitive business environment, more and more leading companies are building new Web-based infrastructures, seeking to gain the strategic advantages of collaborative networking. And they must do this with tightening budgets and stretched resources. But for those organizations that are able to build a collaborative e-business model, the door opens to a wealth of measurable benefits, including:

- **Increased revenue**, by leveraging the Internet for e-sales and other commerce opportunities
- **Reduced cost**, by streamlining supply chains and day-to-day business interactions and processes
- **Improved productivity**, by enabling more efficient collaboration and automating cumbersome tasks
- **Improved marketplace presence**, by extending a company's global reach

Industry studies have confirmed these advantages. According to Information Week's recent report entitled "Information Sharing and Collaboration," companies that collaborate effectively can expect to increase revenue, reduce costs, and improve productivity.¹ These are the cornerstones of success in today's demanding marketplace.

The rush to realize these benefits has been underway for some time. Open, collaborative networking environments that speed both commerce and communication are rapidly replacing decades-old infrastructures.

Securing Shared Resources

Many companies are creating these profitable environments by Web-enabling the business processes that link their employees, customers, suppliers, and partners. To facilitate collaboration, companies first need to identify each network user and which resources each user is authorized to access. Some companies have faced this challenge by building security "front-ends" to applications. These front-ends are individually hard-coded with access policies and each utilizes its own data repository to keep track of legitimate user identities.

Unfortunately, while useful in the short term, this architecture soon becomes a liability to an expanding e-business as its online business processes grow in number and complexity. Before long, the network of heterogeneous security front-ends become inflexible, ineffective, and expensive to maintain. The solution is to centralize security in the Web infrastructure using an identity management system shared by all applications.

Oblix NetPoint: The Foundation of an E-Business Network

Oblix NetPoint™ is a comprehensive, unified identity infrastructure that serves as a cornerstone for an entire e-business network. A scalable, standards-based solution, this enterprise identity management system maintains both the user profile and security policy information for all enterprise initiatives. This enables companies to maintain just one set of user and policy information that all e-business applications access to determine authentication and authorization privileges. Companies need no longer manage static front-ends, multiple security systems, and scattered user data repositories. Oblix NetPoint centralizes the management of all these systems.

Because Oblix NetPoint—with its unique COREid™ enterprise identity management (EIM) solution—places identity management at the heart of an e-business infrastructure, other applications that require access to user and policy information, such as provisioning and password management systems, can be easily integrated into the environment and deployed more quickly. These additional applications reside on top of the Oblix identity infrastructure, effectively leveraging the rich information that resides there. This creates a unified e-business network that is not only secure and scalable, but can also dramatically lower the cost of doing business.

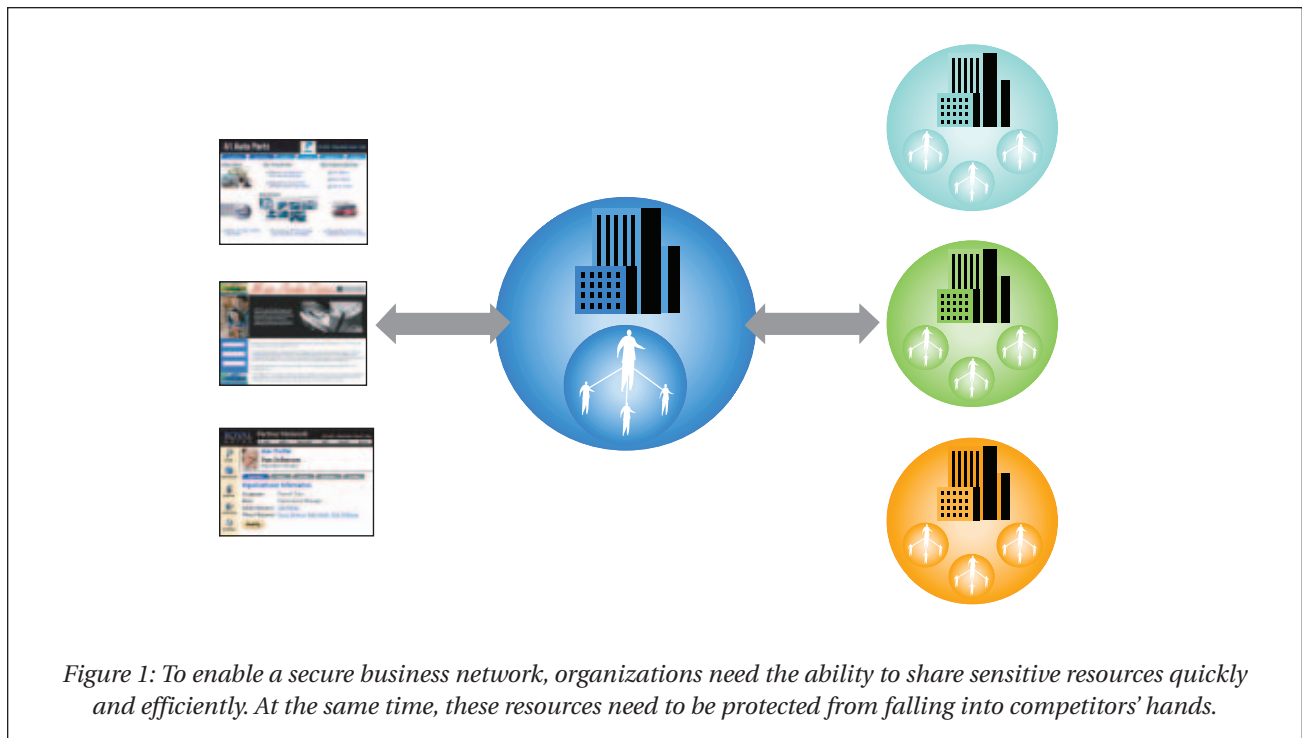
E-business Network Challenges

Managing Complex User Environments

To understand the importance of this identity infrastructure, consider the types of resources that business partners may want to share online. For example, companies linked in an extended, global manufacturing enterprise may profit from sharing a wide range of sensitive resources via the Web: forecasting systems, sales tools and pricing models, ordering histories and systems, customer feedback reports, inventory records, quality reports and defect updates, sales results, shipping reports, customer databases, and even engineering documentation and schematics. In this new open network model, those information assets that were once most closely guarded behind a company's fire-wall are now accessible to suppliers, distributors, customers, and service providers.

While this model provides great gains in productivity and partner collaboration, it also presents heightened security and information management concerns. Clearly, the resources that have the most potential value for a partner would also cause the most damage if they fall into a competitor's hands. An opposite, but equally serious security laps would be an access lockout that accidentally blocks legitimate partners from needed resources.

In essence, the e-business goal is a balance of control: to make information, processes, and systems available without compromising their security.

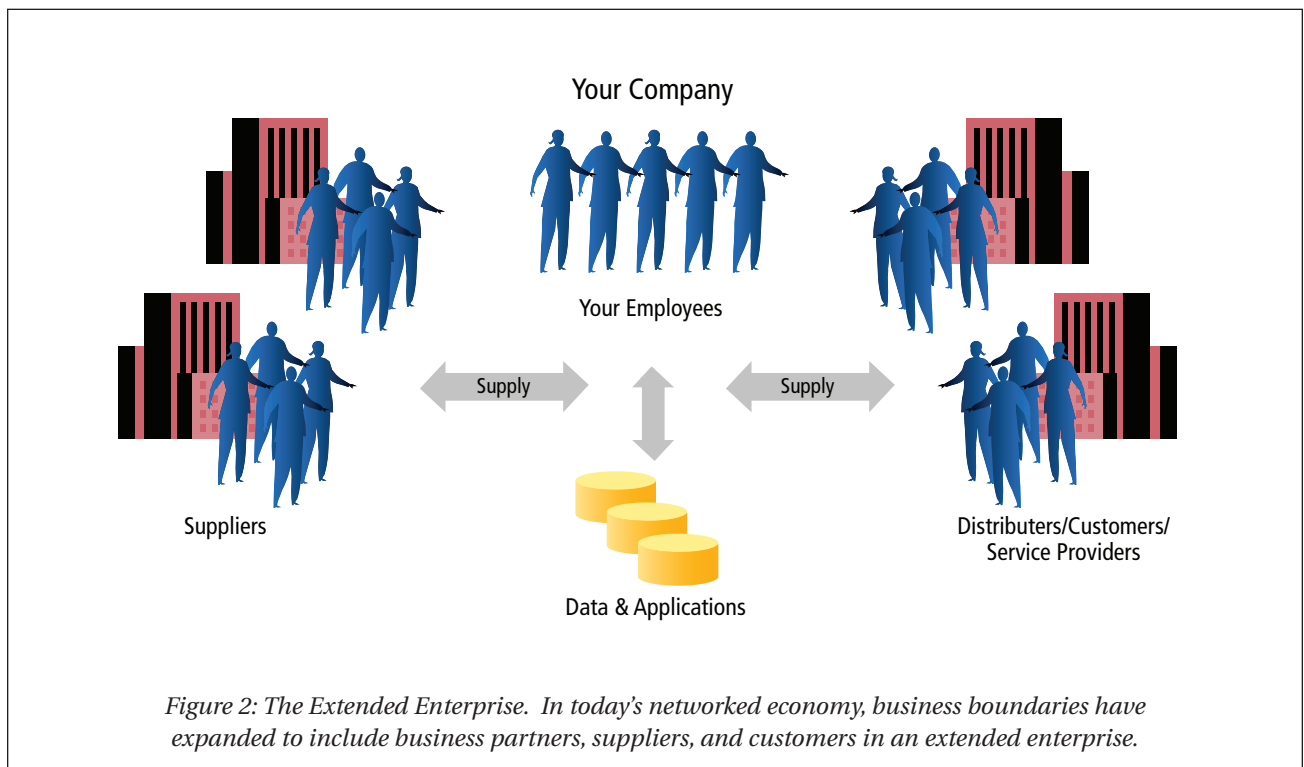


Creating Individualized Access Control

The challenge, therefore, is to manage access to applications and information without canceling the Web's essential value of openness and without creating new administrative or technological bottlenecks. For example, organizations need to give their suppliers access to business applications and data quickly, with a minimum of hassle, so that suppliers can deliver what they need, when they need it. In the process, organizations cannot afford to overload their IT staffs with requests for access by suppliers, dealers, and partners. The answer is to create, for each authorized user in an extended e-business network, an individualized access control scheme that:

- Provides access to all company resources, or only to those resources that an individual needs at the moment
- Can instantaneously extend or block entry into specific resources when either the individual's role or a business initiative changes
- Can immediately and effectively withdraw access privileges when that individual no longer has a legitimate connection to the company

This security model is in sharp contrast to the old system of constructing a firewall to keep "outsiders" out. The new model offers precise, authorized entry to partners with different needs, roles, and levels of responsibility.



Serving Organizations in Continuous Motion

For this system of individualized access control to work, of course, a company must know exactly who should be using its applications and information, and how—minute by minute. Given the size, diversity, and fluid nature of an extended e-business population, this requirement poses both technological and administrative difficulties. Potentially millions of users may be distributed worldwide in thousands of partner companies, and their roles and levels can span all divisions, from manufacturing to sales to engineering to logistics to executive management.

Moreover, each partner organization contributes not only a varied staff of network users with different information needs but also a staff in constant flux. New hires, promotions, resignations, absences, reassignments, and part-time and temporary contracts keep adding, subtracting, and redefining authorized users. For example, over the course of a year in a 10,000-person network, normal business changes could result in as many 350,000 updates to user identity profiles.

New users have to be immediately activated and given access to appropriate information and applications; departing users have to be cut off immediately for security reasons; and information and access rights for continuing users need to be kept current.

In addition, the roles of partner organizations in the e-business network can change with the marketplace. Yesterday's ally can be tomorrow's competitor; yesterday's customer can be tomorrow's supplier. Partners can merge or acquire new businesses. Any Web access management system has to be able to effectively accommodate not only the surge of individual user changes but also large organizational shifts in the value chain.

Several studies support this need for maximum control. According to a recent Meta Group Global Networking Strategies Report, "Global 2000 organizations must enroll and administer customers and internal users quickly and efficiently, or risk alienating users (best-case) or losing customers (worst-case scenario). Mapping IT administration process to key business processes (e.g., hiring, firing, customer contact) can improve service to internal and external customers."²

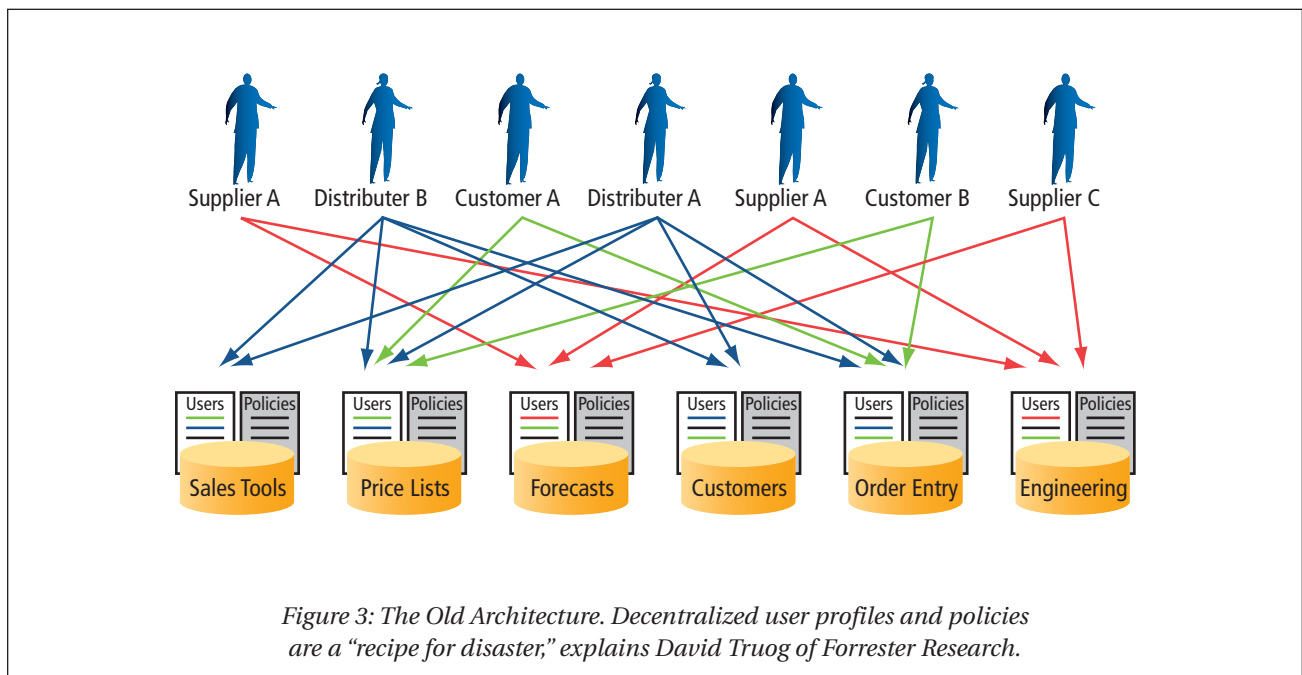
The task then falls to a company's information systems managers to effectively control access to e-business applications and information while maintaining security, keeping costs down, and realizing the significant bottom-line benefits of opening the right resources to the right people in the value chain. They also need an adaptive e-business infrastructure that will scale over time to accommodate growth in users as well as the ongoing delivery of new Web applications and the Web-enabling of legacy applications. The prospect of creating such an infrastructure—and creating it at Internet speed—can be daunting.

Infrastructure Essentials

The right way to establish a secure e-business infrastructure is to deploy a comprehensive enterprise identity management system that:

- Maintains detailed, current identity profiles with information about users' personal credentials and professional roles
- Sets rule-based policies about who may access which resources
- Centralizes all policies and identity profiles in one place for easy, coordinated, and unified management

A unified enterprise identity management system eliminates the inefficiency and confusion of having each application operate and behave independently, with administrators forced to manage disconnected lists of users and access rights with non-standard administration tools. As David Truog of Forrester Research explains it, a decentralized set of controls “is a recipe for disaster,” causing the network to be neither scalable nor secure in the face of constant user changes. With multiple, disconnected lists across applications, “adding or changing customer profiles...requires repetitive, error-prone changes for each app. Efficient access control management must be centralized—out of the apps and all in one place.”³



LDAP (Lightweight Directory Access Protocol) directories have quickly emerged as the standard data store for centralized repository of user identity profile and policy information. This directory server-based architecture is optimized for both security and scalability.

Access Control

With a centralized enterprise identity management system in place, a company can rely on rule-based authentication, access control, and personalization applications to target resources to each user. For example, when an individual playing any role in the e-business accesses a company's extranet site, that person can first be authenticated based on the information in the central directory. Identity at most of today's organizations is established with a username and password stored in the LDAP directory; digital certificates and other authentication mechanisms are also growing in popularity. If there is a match, the authenticated user gains entry. Auditing and reporting applications can track use of resources and alert administrators to anomalies or possible problems.

Second, an access control application can powerfully enforce security policies by checking the detailed role information in that individual's user identity profile, such as title, organization name, department name, function, level, contract details, employment type, and reporting relationship. With this type of context-rich information, the application can leverage a small number of centrally defined policies to grant rights to sensitive applications and data to large numbers of users.

For example, to determine access to a module containing a company's master forecast, the application might verify that the user:

- Belongs to an organization specified as supplying a particular component,
- Works in a department specified as 'manufacturing',
- Has a function specified as 'logistics', and
- Has an employee type specified as 'permanent'.

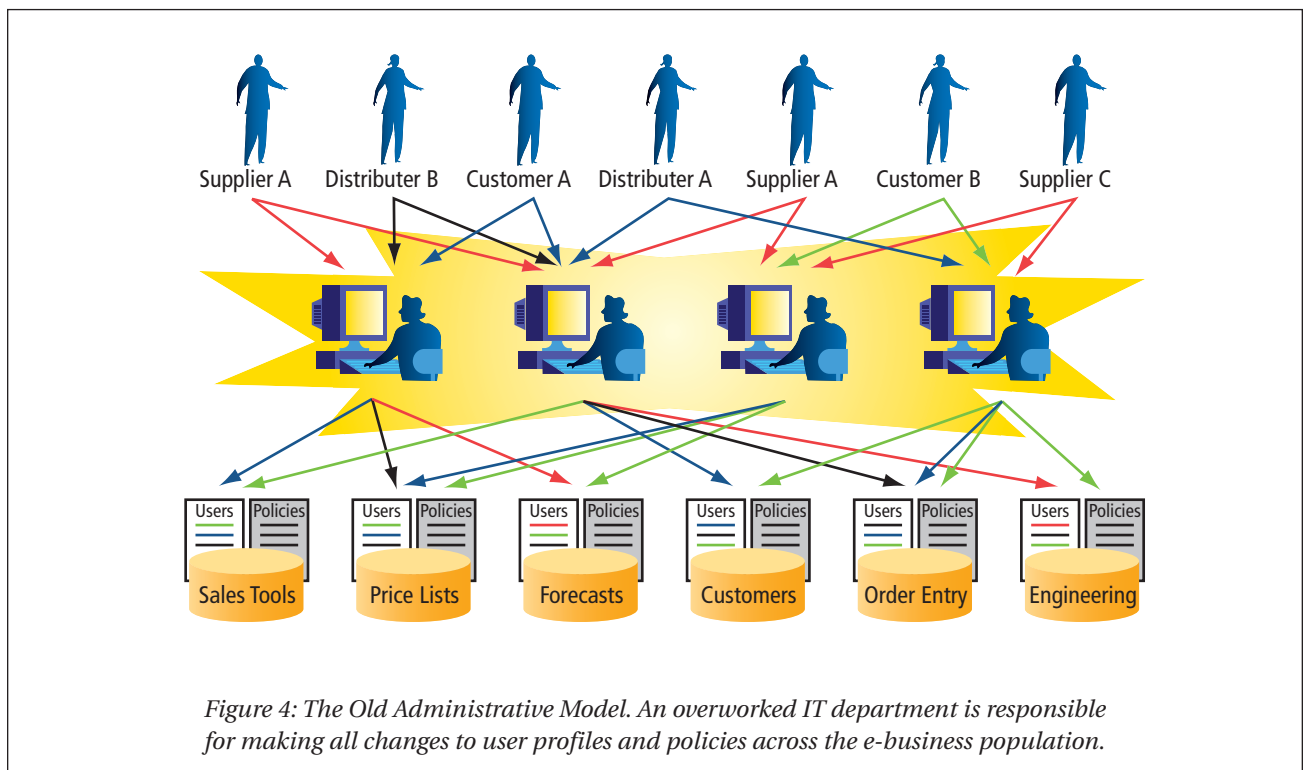
With this role information verified, the application can open this module—and all others that central policies define as necessary and legitimate for this user—with speed, security, and accuracy. Finally, a personalization application can aggregate, package, and deliver to unique Web pages perfectly tailored to the user's needs. Only authorized information is presented, and it is presented in a way that is relevant, appropriate, and useful. The result: a precision e-business tool with no extraneous clutter, with all the necessary resources aligned for efficiency, and with a consistent information interface that expedites decision-making.

Enterprise Identity Management (EIM)

Clearly, the success of this enterprise identity management system depends on the ability to keep the fine-grained information in user identity profiles clean, valid, and up-to-date. This data is the central touchpoint for all authentication, authorization, and personalization decisions and is used minute-by-minute to verify who may see what, based on current role-based policies. Many other types of applications can also be built upon an identity system, such as password management and provisioning systems.

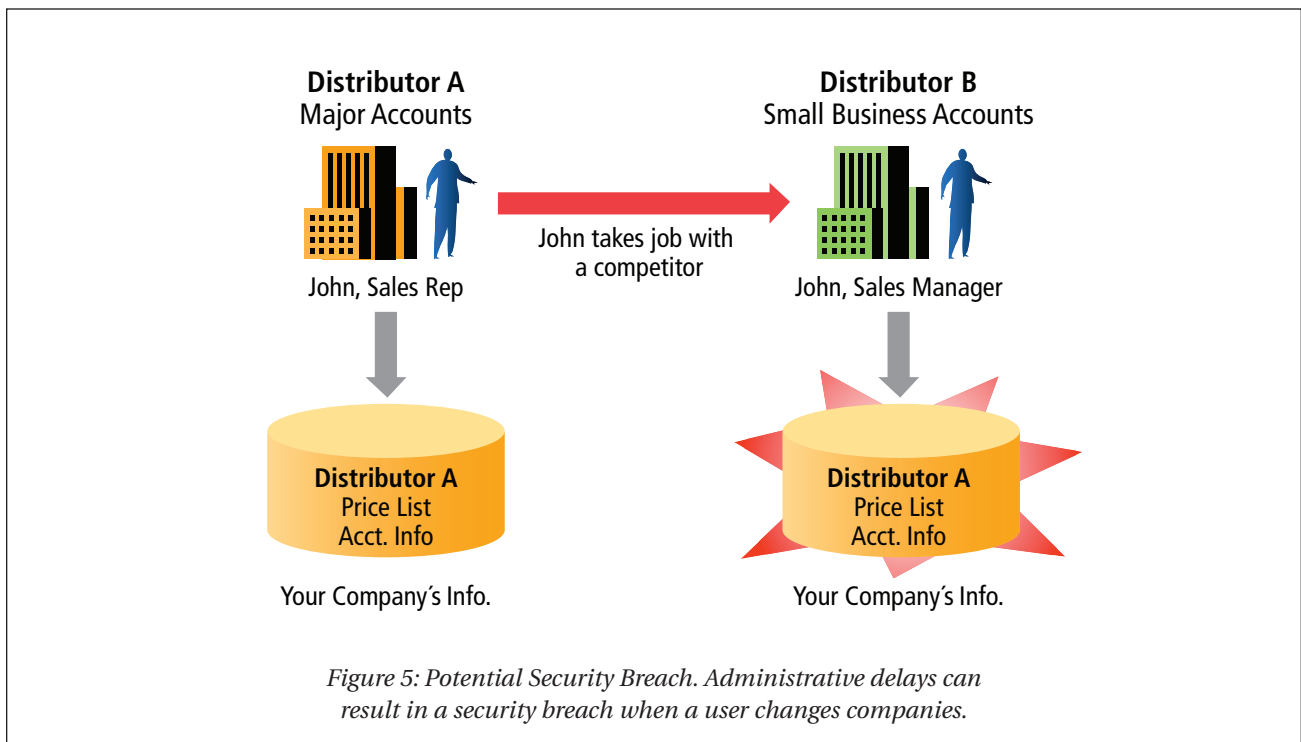
Not surprisingly, user identity is the most accessed information type in the e-business operation. Accuracy is essential. Even the most sophisticated access policies and applications cannot possibly deliver a secure, targeted, personalized e-business network if the user identity data itself are managed poorly.

For example, in the traditional system of Web access administration, one group of central IT administrators in a distributed e-business network is responsible for keeping all user information up-to-date. If an individual wants to change even a minor attribute in her user information, she has to become an active advocate for this revision, either routing a formal approval request through her manager or sending a message directly to the IT person in charge. Similarly, managers have to consistently dedicate time to documenting all user arrivals, departures, and role reassignments and relaying this time-critical profile information to their IT department.



If this time-consuming, often badly coordinated process is allowed to continue, IT administrators must struggle with a steady flow of user changes from myriad sources outside their organization. Severe bottlenecks inevitably occur, as user identity information changes are queued for processing by either the first available administrator or the administrator assigned to a specific account. Either way, IT administrators are forced to operate reactively, without an automated process or a unified view for user identity management.

This model often results in delay, redundancy, and error; business productivity and security are compromised. For example, a company's e-business security is meaningless if administrative overload or oversight allows the profile of a partner's former sales manager to remain active—even after she leaves to join a competitor. Supply chain efficiency is impossible if a newly hired logistics representative in a supplier company is not immediately alerted to an order increase because she has not been authorized to access the master forecasting module. Responsiveness is compromised if a group of users sharing a key attribute—employees of a new shipping partner, for example—cannot be automatically and swiftly authorized. And personalization is out of the question if an administrator is completely in the dark about who a distributor's contract employee is and whether that person needs product margin reports or sales results to do her job.



Scalable Administration

The ability to delegate identity administration to the most appropriate individuals is of paramount importance in developing a collaborative infrastructure that can scale, yet remain up-to-date and accurate. A delegated administration system ensures identity data is approved and maintained by the individuals who are closest to it—and therefore best able to keep it current.

Many growing companies also find it a costly burden to enter thousands of different types of new users into their systems, give them appropriate access privileges, and then handle their ongoing requests and services through traditional administrative processes. Organizing users into groups helps address this problem of scalability by allowing security administrators to place users with similar privilege requirements into a single unit. Once users are organized into groups, administrators can assign access privileges by mapping groups to resources.

This group management approach eliminates the need to individually map each user to each resource, opening the door to a range of benefits:

- Decreased administrative costs
- Increased efficiency
- E-business scalability
- Tighter security

Under a group management solution, new users added to the environment can automatically inherit a predefined set of privileges through assignment to a group. Likewise, a predefined set of users can automatically be given the right level of access to a new application, simply by adding their group to the security policy for the new application.

Because group memberships are directly linked to security privileges, e-businesses set very high requirements for group management. Organizations need a solution that enables groups to be managed effectively, while keeping administrative costs low.

An effective group management solution must also be integrated with a workflow capability to automate data changes and apply business logic to group management. For example, an e-business may want to delegate the ability to create groups to an administrator in an external organization, but may also want to put some administrative checks and data validation processes in place to ensure that the groups created by the external administrator meet certain criteria.

Oblix NetPoint: A Complete Identity Infrastructure

Only Oblix NetPoint provides all these infrastructure essentials in an integrated enterprise identity management and Web access control system. It provides centralized management of user identities and security policies with delegated administration and automated workflow, all delivered in a Web services architecture. Oblix is the leader in identity management and is uniquely suited to provide this foundational infrastructure need.

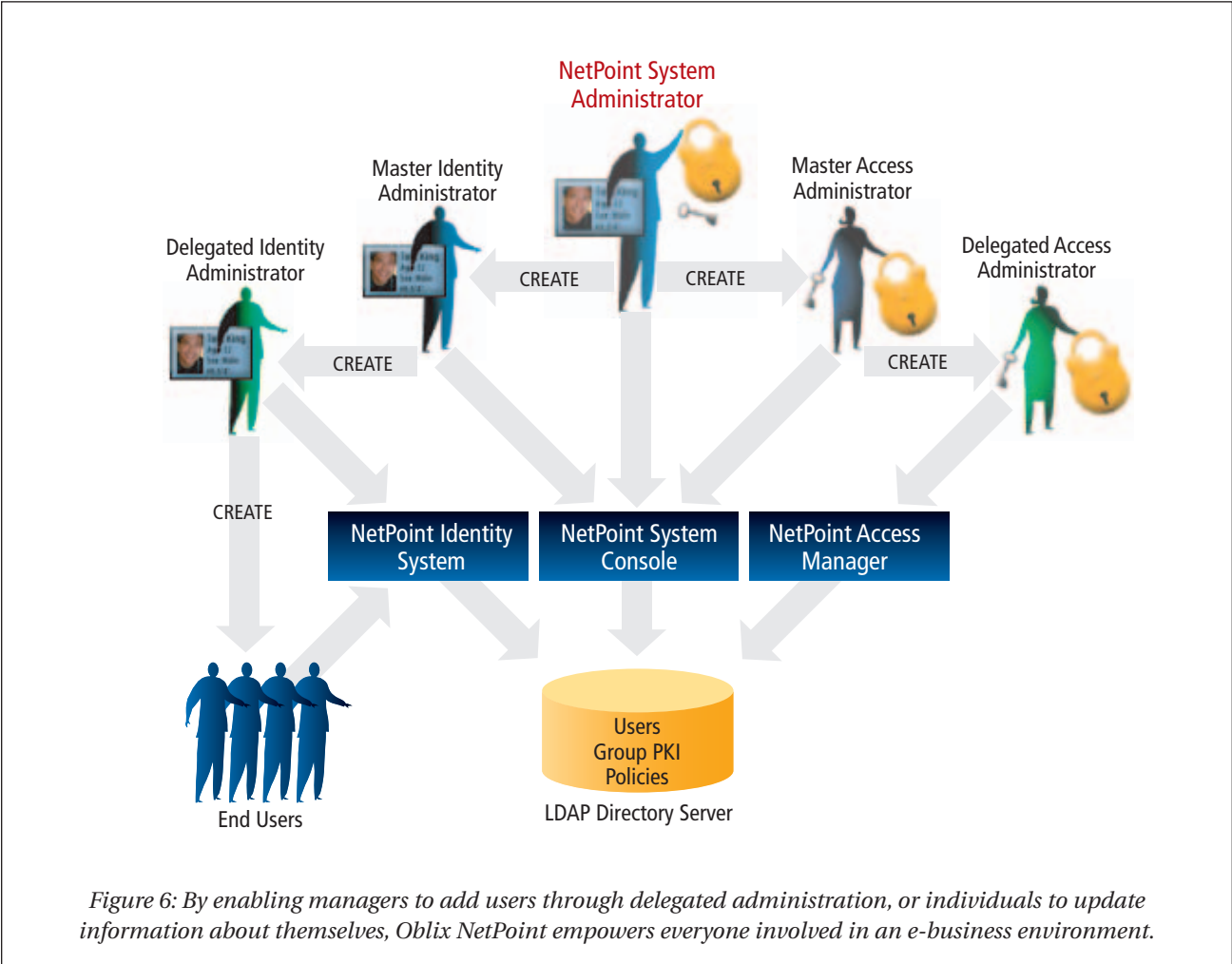
COREid

The NetPoint COREid System™, within Oblix NetPoint, allows companies to dynamically manage identity information about each individual user, group of users, or organization profiled in their e-business network, providing a flexible and secure infrastructure that can manage a maximum number of people at a minimal cost. COREid provides robust user and organization management through a complete range of features that include Delegated Administration, Identity Workflow, Group Management, IdentityXML™, and the FEDERATEDid Layer™.

Delegated Administration

The NetPoint COREid System provides companies with the systems, controls, and practices they need to keep up with the sheer magnitude of changes necessary in a large, diverse, distributed environment. COREid features delegated administration to manage changes to personal identity information—for users, groups, and organizations.

Through delegated administration, COREid distributes the responsibility of maintaining identity information (such as a person's title and phone number) and security information (such as different access rights for tier-1 and tier-2 suppliers) throughout a network of internal and external users. COREid's delegated administration also gives companies maximum flexibility to align EIM practices with their established business processes. For example, COREid allows e-businesses to precisely control which individual attributes different people are allowed to control based on business rules, which interface users see, and even assign temporary responsibilities while personnel are out of the office.



Identity Workflow

COREid’s workflow engine provides an automated way to request and approve identity management changes in large, distributed e-business networks in a manner that supports consistent business rules and processes. Companies can set up customized, easily scalable workflow processes consisting of one or more related steps to implement, approve, and execute tasks that include: user/group/organization Creation, Deletion, and Modification; User Self-Registration, Partner (company) Self-Registration, Subscribe/Unsubscribe to Group; as well as Issue, Revoke, or Renew digital certificates. Because these workflows can be handled transparently via email to internal or external users, e-business constituents do not have to know where to send requests for changes to their identity profiles.

Group Management

The Group Manager application within COREid offers unmatched flexibility in allowing organizations to dynamically manage identity information for constantly changing teams. COREid makes it easy for companies to create, maintain, and delete virtual groups. COREid will list the groups an individual has joined or is eligible to join and allow users to self-subscribe or unsubscribe to these groups. Business leaders, rather than IT, can manage groups. COREid also provides a dynamic framework for rule-based access control that establishes role context in terms of security actions. With these capabilities, e-businesses can eliminate the administrative headache of continually updating individual memberships and enhance security by ensuring that changes in user identity that would automatically disqualify someone from group membership are dynamically reflected in the team.

IdentityXML

IdentityXML, an important feature of COREid, automates change management for large organizations with large numbers of business partners, suppliers, and customers within their network. IdentityXML enables the exchange and synchronization of identity information programmatically through XML over SOAP over HTTP. With IdentityXML, Oblix is the first to deliver to market a means for exchanging digital identity information through Web services. As a result, IdentityXML enables the non-disruptive exchange of identity information within organizations and across corporate boundaries, greatly reducing administrative costs on both sides of the identity exchange.

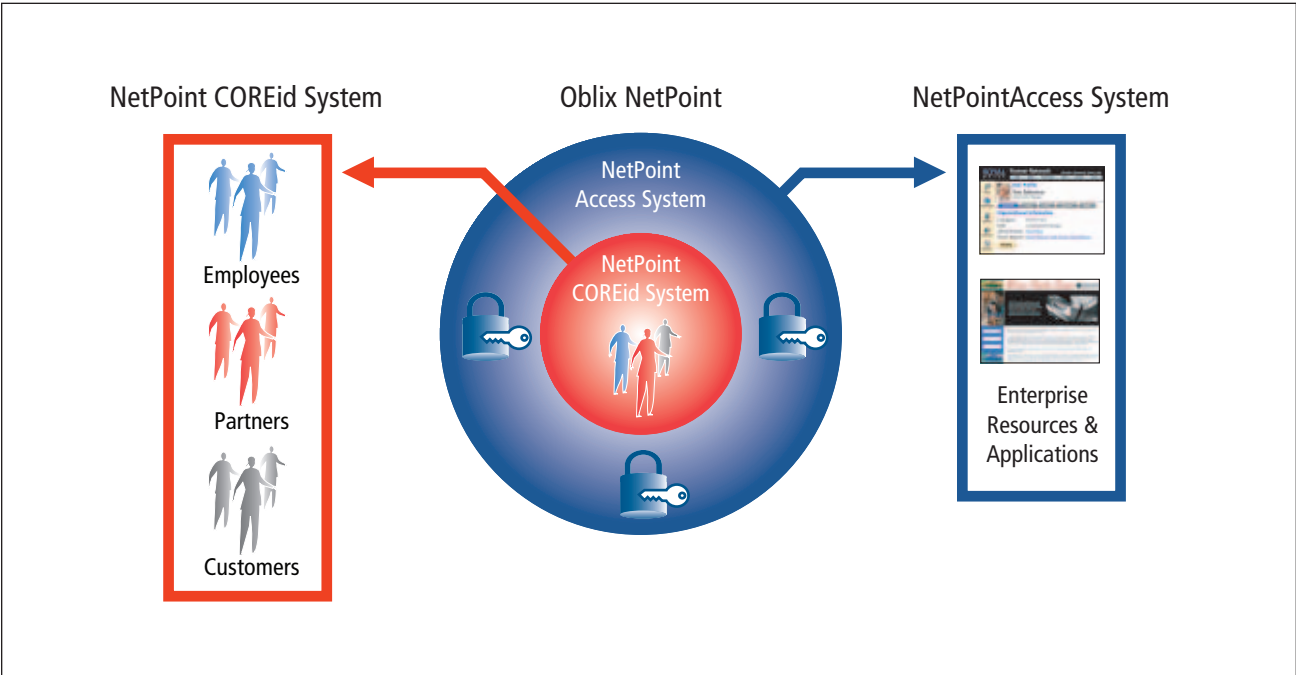
FEDERATEDid Layer

Identity federation enables the sharing of identity-related data, such as authentication information, across multiple trusted business partners. The NetPoint FEDERATEDid Layer is an integration layer that allows a third-party (such as .NET Passport) to provide authentication while NetPoint seamlessly provides authorization and identity management without requiring the user to log-in more than once. With the FEDERATEDid Layer, Oblix allows companies to include as diverse a set of users in their e-business systems as they desire.

Web Access Management

Oblix NetPoint relies on COREid as the foundation for its rich suite of Web access management functionality. This comprehensive set of services and functionality provides robust security for all enterprise systems, whether they are packaged applications, custom-developed applications, or portal products. This Web Access Management functionality includes:

- Authentication to verify identity. Oblix NetPoint furnishes out-of-the-box support for all of the industry's most popular authentication schemes and simplifies user access through single sign-on.
- Authorization to determine access right. Oblix NetPoint offers security policies that enable companies to define the authentication, authorization, and auditing rules for the most flexible and granular protection of enterprise resources.
- Auditing and logging. Oblix NetPoint's comprehensive set of auditing and reporting functions enable organizations to perform security-level auditing of user access to resources as well as business-level auditing and user profiling.



Integration with Web Infrastructure Applications

As the cornerstone for an entire Web infrastructure, Oblix NetPoint is designed for turnkey integration with a wide range of Web infrastructure applications that include provisioning systems and other systems.

Provisioning

Oblix NetPoint provides extranet provisioning for most common LDAP directories. For companies that have not implemented a central directory architecture or that have an existing intranet environment with multiple identity stores, Oblix NetPoint offers Oblix IDLink™ to provide advanced integration with Control-SA® from BMC Software. With the Oblix IDLink for BMC solution, organizations can use the NetPoint GUI to set up, change, and de-activate digital identities and access rights for all users of Web-based and back-end applications throughout the extended enterprise. Organizations can also set up end-to-end self-service and self-registration for both provisioning and user identity management through a single interface.

Integration Services

Oblix NetPoint is the central identity infrastructure that binds all resources and users in an e-business network. It eliminates the inefficiencies of having multiple, disconnected security and user stores for each application server, portal, personalization server, and legacy applications. Oblix NetPoint is designed specifically to work in heterogeneous, mixed vendor environments. Oblix NetPoint provides a wide range of Web services, APIs, and other product components to facilitate seamless integration into a company's infrastructure. With Oblix NetPoint, companies can take advantage of reusable security and identity services that can be leveraged across all applications and users.

Conclusion

Designed to integrate seamlessly with a company's existing applications, systems, and processes, Oblix NetPoint delivers the essential enterprise identity management and Web access control infrastructure required for today's e-business models. The business benefits offered by NetPoint are substantial—and measurable—for organizations building and managing a dynamic e-business. They include:

- **Rapid Return on Investment**—Oblix NetPoint dramatically reduces IT staffing costs by eliminating the manual tasks of maintaining individual user information. Group management keeps critical identity data and access privileges for huge user populations up-to-date. Multi-level delegated administration lets the people closest to user information assume responsibility for its management, improving system scalability. A completely automated workflow engine eliminates administrative workloads and applies business rules consistently throughout a growing enterprise.
- **Stronger Security**—Oblix NetPoint's robust COREid and Access Systems let companies rapidly and consistently manage changes in identity and policy information, eliminating the latency that creates security holes. Oblix NetPoint allows e-businesses to proliferate security policies to their entire network, including applications, portals, and back-end systems. It enables attribute-level access control to allow organizations to develop and apply security policies that map directly to business rules and to apply security policies for granular protection of applications based on security need. NetPoint Federation services enables NetPoint to extend this powerful security protection beyond the enterprise to enable secure collaboration with partners, customers, and other business constituents.
- **Greater Scalability**—Oblix NetPoint was designed for large enterprises planning extensive growth of their e-business operations. Delegated administration means corporations need not scale their IT organizations with the number of users. Extensive caching and built-in failover provide a highly secure, reliable, and scalable deployment. Extensive integration capabilities ensure that enterprise technology investments are well protected and that future technologies can be easily incorporated into the environment.

With these capabilities, Oblix NetPoint provides a comprehensive enterprise identity management and web access control solution that can integrate with an existing network as well as adapt and scale to meet emerging business needs. With the most sophisticated identity management functionality and the highest performance on the market, it delivers the only identity infrastructure able to power e-business for immediate gain and long-term success.

References

1. Information Week Research, “Information Sharing and Collaboration: A Matter of Trust” (5/01).
2. Meta Group, “Global Networking Strategies Report” (5/11/01).
3. David Truog, “Centralize Access Control Now,” Forrester Report (6/99).