



Directory- Powered BusinessSM

**An Introduction to
Identity Management,
Enterprise Directory
Services, and
Directory-Powered
Applications**

An ePresence White Paper

Table of Contents

EXECUTIVE SUMMARY	1
THE CHALLENGE: IDENTITY CHAOS	3
ENTERPRISE DIRECTORY SERVICES AND IDENTITY MANAGEMENT.....	5
Directory Fundamentals.....	5
Toward Enterprise Directory Services	6
DIRECTORY-POWERED APPLICATIONS.....	8
IMPLEMENTATION	9
Implementation Challenges	9
A Deployment Roadmap	10
Leveraging the Initial Project.....	12
FOR MORE INFORMATION	13

February 2002



Unleashing Directory-Powered BusinessSM

Corporate Headquarters
120 Flanders Road
P.O. Box 5013
Westboro, MA 01581-5013
Tel: 508.898.1000
info@epresence.com
www.epresence.com

©ePresence 2002. All rights reserved. All information contained within is a copyright of ePresence, Inc. ePresence and “Unleashing Directory-Powered Business” are servicemarks of ePresence, Inc. All other products or companies referenced herein are registered trademarks of their respective companies.

Executive Summary

Today most business processes depend on information technology systems. Employees need reliable, convenient access to applications and data to do their jobs. Customers and business partners must be granted fast, secure access to web sites so they can query, collaborate and buy. At the same time, enterprises must protect information assets from internal and external threats.

The Challenge: Identity Chaos

Unfortunately, in most organizations information about system users and their rights to access and use applications is fragmented and duplicated across many applications, databases, and directories. And every day employees arrive, change roles and leave, new applications come on-line, and new customers and business partners collaborate, order and ship.

As a result of this “identity chaos,” most organizations are severely challenged to provide reliable, secure access to applications and data. Enterprises see productivity fall, costs increase, and new business initiatives falter. And “orphan” user accounts expose organizations to potentially disastrous breaches in security.

Directory Services

A directory manages information about people who use information resources and their rights to those resources, including:

- Identity
- Authorization to access specific resources
- Passwords and security parameters
- Personal information and preferences.

When implemented across an organization, “Enterprise Directory Services” (or “eBusiness Directory Services”) provide a single logical resource to manage user identity, access, security and preferences information. As shown in Figure 1, this answers the needs of three audiences:

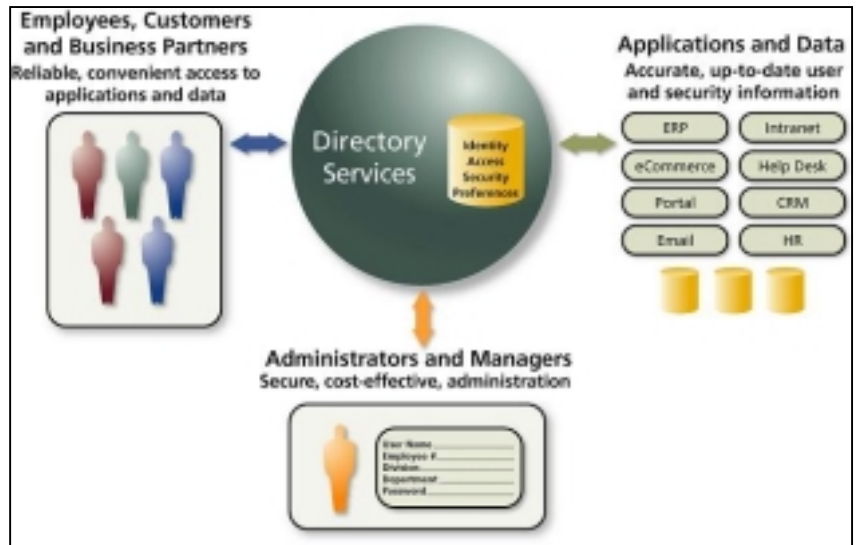


Figure 1: Directory Services Provide User Information to Systems Users, Applications, and Administrators

System Users. Employees gain reliable, convenient access to applications and data. External users can be granted secure, flexible access to information and collaborative tools.

Applications and Application Developers. Applications obtain up-to-date information on users and permissions from a trusted source, while application developers don’t need to recreate user management and security functionality in every application.

Administrators and IT Staff. Administrators and the IT staff can manage the torrent of changes in users, applications and systems, while applying coherent security policies.

Enterprise directory services can have a material impact on the effectiveness and efficiency of an organization:

- **Productivity increases**, because employees have reliable access to applications and spend less time worrying about passwords and sign-on procedures.
- **eBusiness and supply chain initiatives are more successful**, because customers and business partners can conveniently and securely utilize applications and collaborate with employees.
- **Costs are reduced**, because the IT staff can manage user and permissions information from a single point.
- **Security is improved**, because security policies are applied quickly and consistently across the entire IT infrastructure.
- **Marketing and customer service become more personalized**, because customer preference information can be stored and accessed centrally

Directory-Powered Applications

An organization that has established reliable directory services can further increase the return on its investment by implementing one or more “directory-powered applications” such as **web single sign-on, provisioning, portals, and personalized marketing**. These applications leverage user information managed by directory services to provide secure, personalized services to employees and outside parties.

Implementation Challenges

While enterprise directory services provide far-reaching benefits, implementation requires time, effort and careful planning. It is necessary to address business objectives and priorities, organizational issues, security policies, technology options, systems integration, and user and administrator training. The best results are likely to be achieved through a comprehensive process such as the ePresence “Roadmap,” a methodology with four distinct phases: **Strategize, Visualize, Realize, and Optimize**.

This White Paper

Our goal in this white paper is to discuss the factors behind “identity chaos,” to describe the solution--enterprise directory services, to touch on “directory-powered applications,” and to outline the type of implementation process that can ensure a successful result.

If you have any questions or comments, we would be very pleased to hear from you at: info@epresence.com.

The Challenge: Identity Chaos

To provide services while preserving security, IT applications and systems need to know the identity of each user. And additional information about users can help some applications provide personalized services. The type of information useful to an application might include:

- Who is this person? (Identity)
- Is this person really who he or she claims to be? (Authentication)
- Is this person authorized to use this resource, or certain parts of it? Only to see information, or also to make changes? (Access Control or Permissions)
- Does this person belong to a group or fulfill a role that has been granted or denied specific privileges? (Roles and Policies)
- Is there information about this person that would help me provide customized services? (Preferences)

Challenge: Redundancy and Inconsistency

Unfortunately, in most organizations this information is fragmented and duplicated across many applications, systems, databases and directories (Figure 2). In fact, a study by the industry analyst firm Giga Group found an average of *over 80* directories and user data stores in a typical large corporation. Further, the identity information is usually expressed inconsistently across the system—“William Smith,” “Bill Smith,” “Bill H Smith” and “W.H. Smith”—making it impossible to provide a complete picture of this person’s activities. And each system has its own security procedures and passwords and its own definitions of user groups and roles.



Figure 2: Identity Chaos: User Information Fragmented and Duplicated, Constant Change, New Challenges

Challenge: Maintaining Security in the Face of Constant Change

Constant change is a fact of business life. Every day new employees are added, change roles, and leave the organization. New customers and partners appear, change in status, and disappear. Each of these internal and external users must be identified in multiple systems, and have access privileges granted or removed throughout the life cycle of that person’s relationship with the organization. And user permissions need to be adjusted as applications, servers and networks are added, upgraded and removed.

Challenge: Supporting New Business Initiatives

IT groups are also being challenged to support new business and technology initiatives: streamlined business processes, innovative new services for customers, supply chain integration, new web and wireless technologies. These initiatives require storing new types of information about users and demand even higher levels of reliability and consistency in controlling access and maintaining security.

The Costs of Chaos

The factors discussed above typically result in “identity chaos,” where user information is fragmented and duplicated, system users must remember multiple passwords and sign-on procedures, obsolete information is rampant, and security is problematic. This state of affairs can have a direct impact on the effectiveness and profitability of the organization. For example:

- **Productivity falls**, because employees waste hours waiting to obtain access to applications, logging onto multiple systems, and calling the help desk to reset passwords.
- **eBusiness and supply chain initiatives falter**, because customers and business partners find that access to applications and collaborative tools is not reliable.
- **Costs increase**, because administrators spend hours entering duplicate information in multiple systems, and the help desk spends days retrieving passwords for users.
- **Security is compromised**, as obsolete information and “orphaned” user accounts provide avenues of entry into enterprise systems.
- **Application rollouts are delayed**, as developers re-create user management and security functionality in each application.
- **Marketing and customer service fall behind competition**, because customer preferences can’t be shared across systems.

Enterprise Directory Services and Identity Management

Enterprise directory services provide a solution for the problems of “identity chaos.”

Directory Fundamentals

At the most basic level, a directory is a repository of information about users, applications and networked resources. Most of the information is focused around topics such as:

- Identity
- Access
- Security
- Preferences

Identity information may include the user’s name, nicknames and aliases. It can also include groups or roles to which the user belongs, such as “management,” “contractor,” or “distributor.”

Access information may include permissions to use specific resources or classes of resources, including applications, databases, web sites, servers, output devices and network links. It can also specify rights pertaining to those resources, for example to view, add, modify or delete data.

Security information may include parameters related to user authentication, such as passwords selected by the user or by an administrator. The directory can also be used to store digital certificates used by PKI (Public Key Infrastructure) and other security schemes.

Preferences consist of information submitted by the user, or inferred from the user’s behavior on a web site, that can be used to personalize services. Preferences can be stored in a directory or in another data store interfaced with the directory, and made available to other applications.

Administrative Tools

A directory typically provides tools for the administrator to add and manage user and resource information efficiently. Management procedures are streamlined, because the administrator can work with many users at once through the use of groups and roles. For example, the administrator may be able to give the entire finance department access to a new application, or specify that only employees in a “management” role can use a certain human resources function, or connect distributors in Europe to a local price database.

Similarly, a directory can allow administrators and support personnel to view and modify security settings and passwords quickly and easily. The directory may even be able to synchronize passwords across multiple applications without any intervention from the administrator.

Directories can enforce a centralized style of management, giving the central IT group tight control of changes, or support a decentralized model by delegating specific powers to local administrators.

Finally, a solid directory can be invaluable for migrating between software products or to newer versions of a product. For example, it can facilitate the bulk modification and transfer of user information while upgrading a desktop operating system, or in converting from one email package to another.

Application Interfaces

A directory is also a resource for applications and other elements of the IT infrastructure. Applications can access the directory for accurate, up-to-date user identity information and for user authentication. Infrastructure and middleware products that join information across applications can use a directory to establish the identity of users across systems.

In addition, there are a number of “directory-powered” applications and services that rely on a directory to carry out their main functions. These include web single sign-on (SSO), provisioning, portals, and personalized support and marketing. These will be outlined in the next section of this white paper.

Toward Enterprise Directory Services

Enterprise Directory Services can be described as a single logical repository of user and permissions information that is available to system users, administrators and applications within and outside the organization (Figure 3).

Enterprise directory services, together with related “directory-powered applications,” can provide a vastly simplified environment for system users, administrators and applications.

Employees, customers and business partners gain:

- The convenience of fewer sign-on procedures and passwords.
- Increased productivity from faster access to applications and resources.
- Improved customer service and collaboration, as employees, customers, partners, customer service representatives, and support personnel all obtain rapid, reliable access to necessary systems and information.
- The opportunity to receive personalized service because user preference information is widely available to applications.

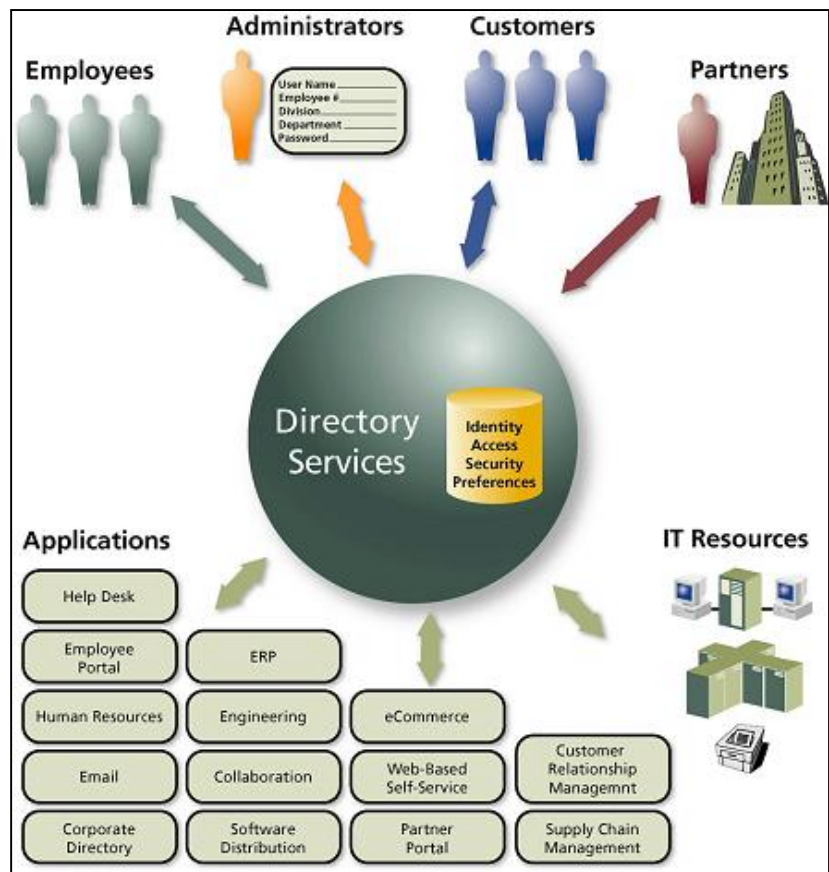


Figure 3: Enterprise Directory Services: A Single Repository of User Information for Employees, Administrators, Customers, Partners and Applications

Administrators gain:

- One place to add, modify and delete user and resource information, or to delegate these powers, with the assurance that changes will be leveraged throughout the IT environment.
- Specialized tools to manage user identities by groups, roles and other aggregations.
- Tools to manage security and “de-provision” employees, customers and partners who are no longer authorized to use systems.

Applications and application developers gain:

- Improved data accuracy and integrity, through the ability to call on a reliable, up-to-date source of user information.
- Accelerated application development and deployment times, since user management and security functions can be off-loaded to directory services rather than re-developed on an application-by-application basis.

Physical Implementations and Meta-directories

Of course, while enterprise directory services provide a simple *logical* view of user and permissions information, the underlying *physical* implementation may be complex. It is rarely practical to replace all of the existing directories in an IT environment with a single, centralized master directory. Accordingly, the physical implementation of enterprise directory services is likely to include one or more of the following:

- Distributed directories from the one vendor.
- Heterogeneous directories from multiple vendors.
- A meta-directory or virtual directory.

A “meta-directory” is a master directory that aggregates information from multiple directories and stores a central copy. A “virtual directory” does not physically store user information itself, but maintains pointers to the relevant data in the separate directories and databases.

Acceptance by the Market

Improvements in directory products, and recognition of their value, are leading to widespread acceptance in the marketplace.

The accompanying chart from Giga Information Group indicates that half of the enterprises surveyed have deployed or are planning to deploy corporate directory services, and that this percentage will increase to 90% by 2004.

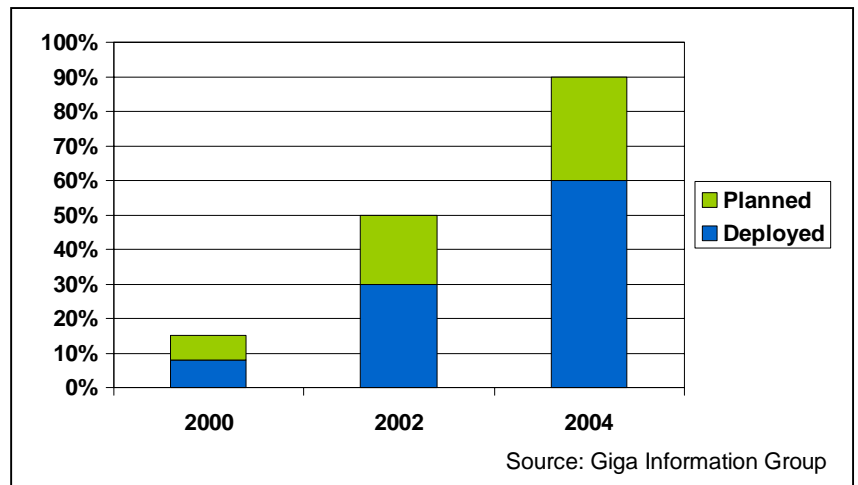


Figure 4: Percentage of Enterprises Deploying or Planning to Deploy Corporate Directory Services

Directory-Powered Applications

There are a number of extremely valuable software applications that are difficult or impossible to manage without accurate and up-to-date user information. However, once an organization has established reliable directory services, it can usually implement these “directory-powered applications” with relative little incremental investment. Figure 5 illustrates how some of these applications can be built on directory services.

Web Single Sign-On (SSO)

Web single sign-on allows an employee, customer or business partner to sign on once, using a single password, and access all authorized applications. This dramatically improves the experience of the user. It also greatly reduces IT support costs related to retrieving and resetting passwords. The web single sign-on service relies on directory services to manage and synchronize identity and security information across all of the user’s applications.

Provisioning

Provisioning uses business rules and workflow processes to allocate access rights and physical resources to employees, customers and business partners. Later it helps modify and “de-provision” access. Provisioning can be initiated by an administrator, or by a user from a “self-service” interface delivered through a browser. Provisioning applications rely on directory services to identify and manage the resources that are appropriate to each user, and to help apply roles and policies to the provisioning process.

Portals and Web-Based Applications

A portal provides a user with a single point of entry to all of the applications needed by that user. Portals can address the needs of employees, customers, and supply chain partners for access to corporate information, transactional systems, external news sources, and collaboration and support tools. Portals use directory services to track the applications authorized for each user, to help authenticate users, to provide personalized screens and applications, and to “push” corporate information to targeted groups.

Personalized Marketing and Support

Personalized marketing and support applications utilize user preference information to deliver customized marketing appeals and to provide access to appropriate information sources and support forums. These applications rely on directory services to track the applications and resources authorized for each user and to store user preferences that can be used to customize messages, information and resources presented to the user.

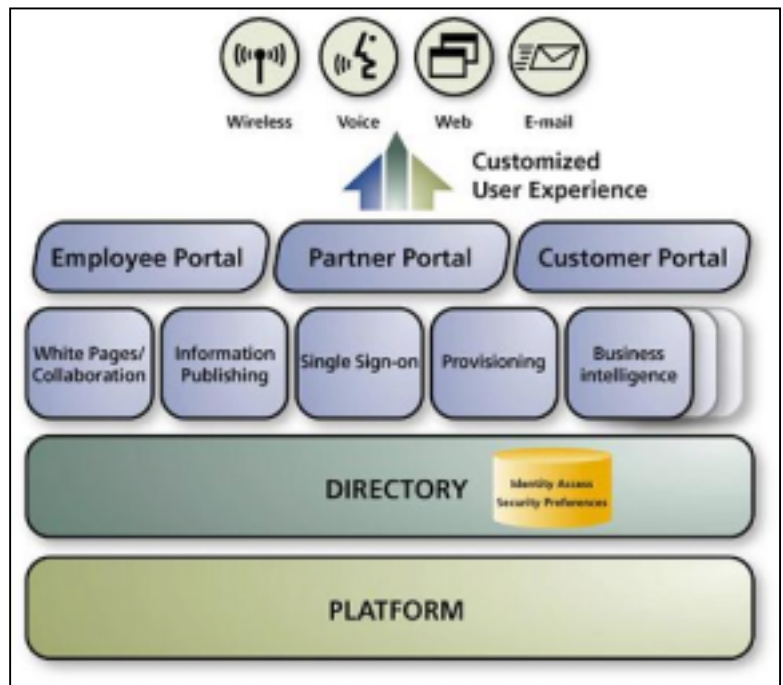


Figure 5: "Directory-Powered Applications" Built on Directory Services

Implementation

Implementation Challenges

While enterprise directory services provide far-reaching benefits across a wide range of applications and user groups, implementation requires time, effort and careful planning. Implementation goes far beyond installing software, and encompasses issues of business objectives and policies, priority setting, technology selection and integration, and user and administrator training.

Challenge: Business Objectives, Policies and Politics

It takes time to deploy directory services across an enterprise. By setting priorities and establishing phases that reflect business objectives, it is possible to realize a solid return on investment for each segment of the project rather than waiting until the end.

Also, because enterprise directory services cut across departmental and geographical boundaries, it is important to design an implementation process that recognizes in advance organizational politics and legitimate concerns about ceding responsibilities to a central group. Educating business and technical leaders on the purpose, value and requirements of the directory project can be critical to a successful implementation.

And because directory services incorporate business policies in areas like security, application access, information sharing, and government-mandated privacy, it is important to understand these issues in advance and address them explicitly in the design of the project.

Challenge: Technical Design

Technical design and architecture are central to a directory services project. It is important to understand the existing directory, application and networking environment, and to select the right technologies in terms of directories, meta-directories and related products. Further, the eventual performance and reliability of the directory service will depend on making sound decisions about architectural issues, such as how to distribute the directory and application components and how to manage communications among them.

Challenge: Installation and Integration

Installation challenges go well beyond merely installing the core directory technology. Directory and security parameters need to be set according to design and business requirements. And invariably the project includes substantial systems integration work to provide the connections between directory products, applications and other elements of the IT infrastructure.

Challenge: Staffing

Staffing issues create special challenges during a directory services implementation, because the project is both knowledge- and labor-intensive. The project requires a wide range of skills that are in short supply in most organizations, including business analysis, system design, project management, systems integration, application development, and a detailed knowledge of directory concepts. Peak periods create a spike in demand for technical manpower that may be hard to meet from the existing resources of the IT department. And as directory services become a core element of the enterprise infrastructure, someone must take ownership of processes to manage the directory and integrate applications and services on an on-going basis.

A Deployment Roadmap

Overcoming the challenges inherent in the implementation of directory technology requires a step-by-step process that fully addresses business, technical, management and people issues.

The “Roadmap” discussed below has been developed by ePresence based on experience with hundreds of large and small organizations. While the final deployment plan will vary widely from situation to situation, this generic version illustrates the type of process that can help you achieve the full benefits of an enterprise directory services project.

This implementation roadmap is based on four phases, linked by project management and other management and training activities (Figure 6).

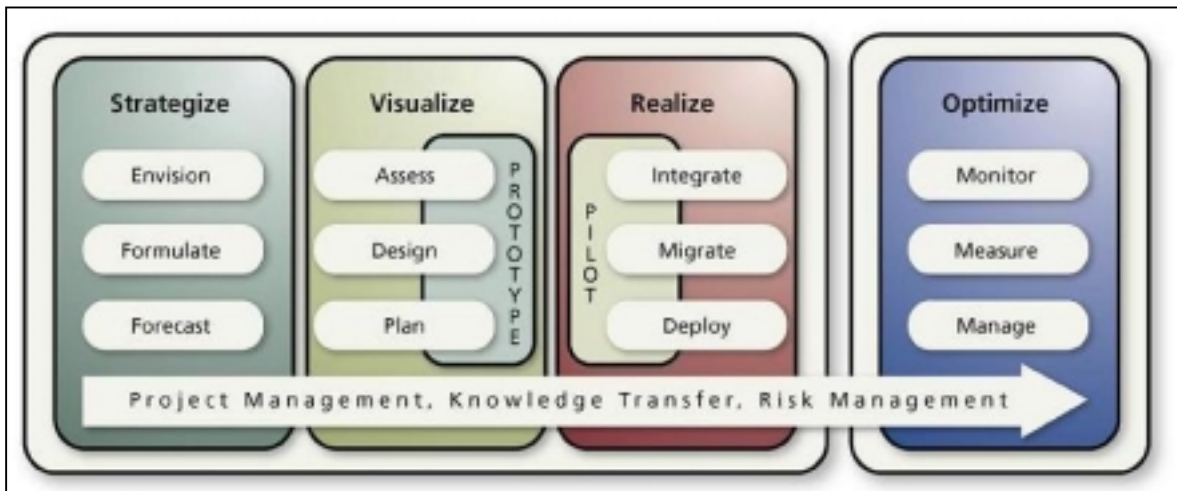


Figure 6: The Four Phases of ePresence's Implementation Roadmap

Phase 1: Strategy Definition

The first phase in a typical deployment plan defines a strategy for the project. This involves understanding the strategy of the enterprise as a whole, and establishing agreement about how that strategy relates to the objectives of the directory services project. This activity requires the participation of many line-of-business and technical groups. Establishing a unified strategy from the start minimizes the political objections that often interfere with a project.

Activities involved in defining the strategy include:

- Determining business, technical and operational goals from both a tactical and strategic perspective.
- Defining directory service requirements at a high level and setting priorities, covering topics such as platforms, connectivity, APIs, support for standards, basic services requirements, security, and administrative and operational capabilities.
- Exploring the roles of technical groups and business units participating in the project.
- Defining the scope of the project
- Outlining a phased approach and milestones to provide incremental benefits and provide management benchmarks.

Phase 2: Detailed Requirements and Solution Design

The second phase of the project translates the strategy into detailed functional and technical requirements and designs the solution. Outputs include a comprehensive deployment plan, final decisions on technologies and products to be used, a budget, and agreement on metrics for success.

Activities related to establishing detailed requirements include:

- Creating a project baseline by assessing the current environment.
- Performing a detailed Business Requirements Analysis that defines business and functional needs in depth and identifies related technology initiatives within the organizations (for example, an ongoing security initiative).
- Developing detailed technology requirements.
- Identifying data sources that need to interface with directory services, as well as requirements related to those data sources regarding security, access control, privacy, provisioning, and data synchronization.

Activities related to planning and designing the solution include:

- Selecting directory and meta-directory products and vendors. This is based on considerations such as performance, scalability, product maturity, replication capabilities, and support for standards such as LDAP, XML, and DSM.
- Designing the Directory Service structure, addressing issues such as the namespace, the schema, information distribution through replication and referrals, user and management interfaces, data synchronization, and provisioning policies and procedures.
- Defining integration and synchronization with databases, applications, and existing directories.
- Specifying security and authentication policies covering topics such as password management, authentication, encryption, read/write/delete access, electronic signatures, certificate issuance and revocation, logging and audits.

Phase 3: Implementation

The third phase of the project is physical. Activities in this phase include:

- Installation and configuration of directory services and related software.
- Specification and configuration of access, security, data replication, management and operational policies and procedures.
- Development of standards for performance, reliability and accessibility.
- Integration with data sources, applications and IT infrastructure components.
- Migration of user, account and resource information from existing directories and data sources to the new directories.
- Testing of individual systems and the complete environment.
- Training and deployment to the target audiences.

These activities may be accompanied by the creation of a pilot system used to demonstrate and test the functionality and performance of the solution for a limited number of users.

Phase 4: Optimization

The fourth phase of the project is Optimization. Typically directory services projects expand in scope over time, adding new users and new applications, so it is important to measure results and reconfigure resources periodically in order to continue to provide a high level of service.

Optimization activities can include:

- Monitoring performance, measuring reliability and accessibility, and comparing results against standards and pre-established baselines.
- Fine tuning architectures, configurations and policies.
- Upgrading software and systems.
- Integrating new applications and data sources.

In addition to performing optimization activities, ePresence can also provide operations management services and take over the day-to-day administration of directory services and related systems.

Leveraging the Initial Project

Organizations typically undertake directory services projects for one of three reasons:

1. To provide a rock-solid foundation for a critical application or set of applications
2. To solidify the information technology infrastructure across the entire enterprise in order to improve productivity and reduce costs
3. As part of the implementation of a “directory-powered application” such as single sign-on (SSO), provisioning, a portal, or interactive marketing and support

However, many organizations have found that they are able to leverage the work done in an initial project to provide additional benefits at a relatively low incremental cost.

For example, an organization might expand the use of directory services from an initial set of applications to additional applications, or across the entire enterprise IT infrastructure. An organization that has built a core directory services platform can easily build additional “directory-powered” applications on top of that platform. Or an organization that has focused on providing convenient access and reliable service to employees can transfer the same benefits to external eBusiness users such as customers and supply chain partners—or vice versa.

For More Information

ePresence has over 18 years experience designing and implementing enterprise directory services solutions and “directory-powered applications.”

Our staff has the complete range of skills needed to ensure the success of a directory services project, including business analysis, project management, information systems design, directory implementation, security, systems integration and eBusiness application development.

Through dozens of project life cycles we have developed a proven directory services implementation methodology and a comprehensive set of service packages, listed in Figure 7.

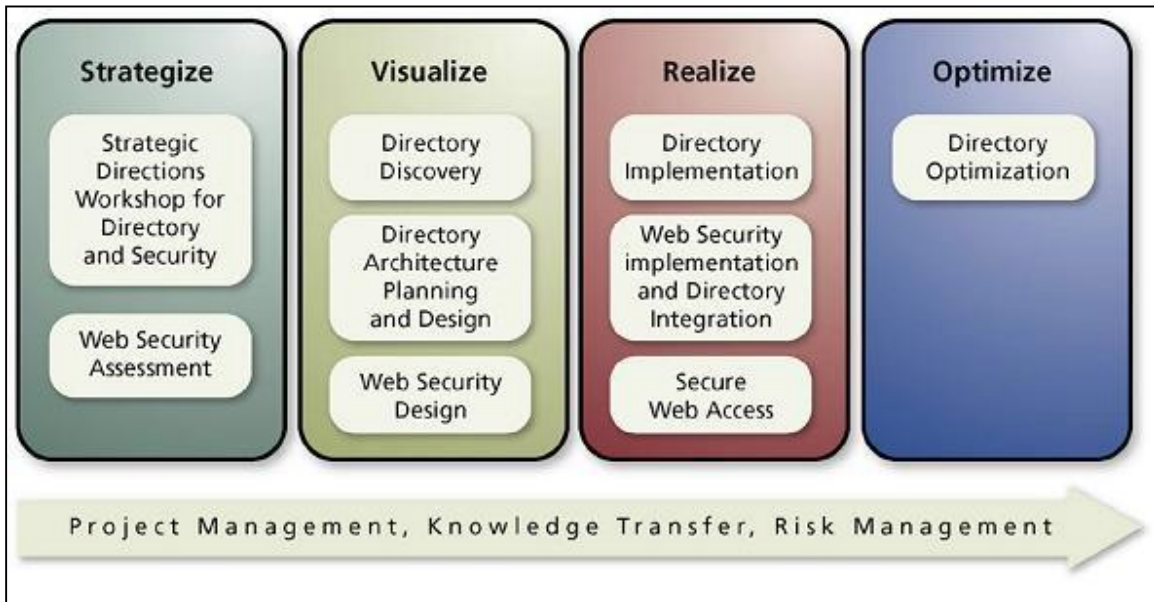


Figure 7: ePresence Service Packages for a Typical Enterprise Directory and Security Services Project

And as a recognized leader in this field, ePresence has been able to form unique alliances with major platform vendors such as Microsoft, Sun/iPlanet, and IBM, as well as partnerships with key technology providers in areas like security, access management, meta-directories, provisioning, portals, application servers, personalization engines and content management.

So for more information on directory services, directory-powered applications, and how ePresence can help you design and implement enterprise directory services, please contact us at 508.898.1000 or info@epresence.com, or visit us on the web at: www.epresence.com.