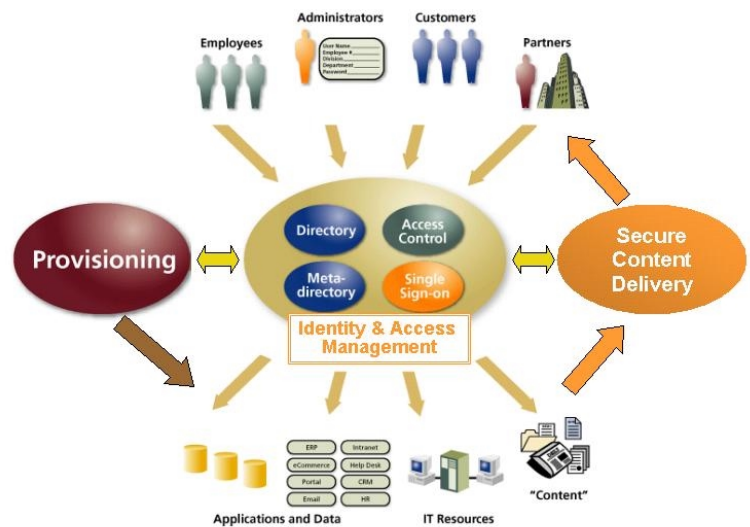




An Introduction to Secure Identity Management



An ePresence White Paper

Table of Contents

INTRODUCTION: ACCESS AND SECURITY	1
THE IDENTITY MANAGEMENT CHALLENGE	2
WHAT IS SECURE IDENTITY MANAGEMENT?	4
A SECURE IDENTITY MANAGEMENT FRAMEWORK	5
Identity and Access Management Services	5
Provisioning	7
Secure Content Delivery	8
RESULTS.....	9
WHERE DO YOU START?	10

Version 2.0

July 2002



Delivering Secure Identity Management Solutions

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 is a servicemark of ePresence, Inc. All other products or companies referenced herein are registered trademarks of their respective companies.

Introduction: Access *and* Security

For information systems to be effective, people must have *access* to computer applications, data and documents.

For information systems to be *secure*, access must be denied to those who might harm the interests of the enterprise.

So it is a fundamental need of information systems to balance access and security by controlling:

- **Who** is allowed to use its information systems,
- **What** information resources each person can access, and
- **How** each person can use those resources.

But giving the right people access to the information resources they need is not a simple matter. An enterprise must develop *policies* about who is entitled to access resources. It must have *processes* to request, approve, grant and revoke access. And it needs *systems* to manage the processes and enforce the policies.

Unfortunately, in most enterprises the systems to control access are fragmented, duplicated, and inefficient. Security policies are enforced inconsistently or not at all. A small army of administrators and help desk personnel labor ceaselessly to update user information and passwords. New employees, customers, and partners wait days or weeks before they are set up with the systems they need to perform work or do business with the organization.

So enterprises are being forced to ask questions like:

- ? Are we confident that we can open our information systems to customers, suppliers and business partners without compromising security?
- ? Are the high costs of user administration and support undermining our budget?
- ? Does inefficient “onboarding” of new employees and contractors erode productivity?
- ? Are we exposed to security breaches if we can’t terminate access in a timely manner?
- ? Can we meet audit and regulatory requirements to protect confidential information?

To answer these questions, many enterprises and industry analysts are systematically re-examining how to optimize the systems and process used to control access to information systems. The result is the emergence of a new discipline: “Secure Identity Management.”

In this white paper we will:

- Discuss why identity management is so challenging today.
- Introduce Secure Identity Management, the new discipline for addressing these challenges.
- Present a framework for organizing the related systems and processes.
- Suggest how you can get started on the road toward Secure Identity Management and quickly begin producing results.

The Identity Management Challenge

In most enterprises today, each individual application or system has its own user database or directory to track who is permitted to use that resource. Each has its own definition of the user's "identity" (name, title, ID numbers, roles, membership in groups). Many have their own password and process for authenticating users. Each has its own tool for managing user accounts, and sometimes dedicated administrators responsible for this task.

Further, most enterprises have multiple processes for requesting resources and for granting and changing access rights. Some of these are automated, but many are paper-based. Many differ from business unit to business unit even when performing the same function.

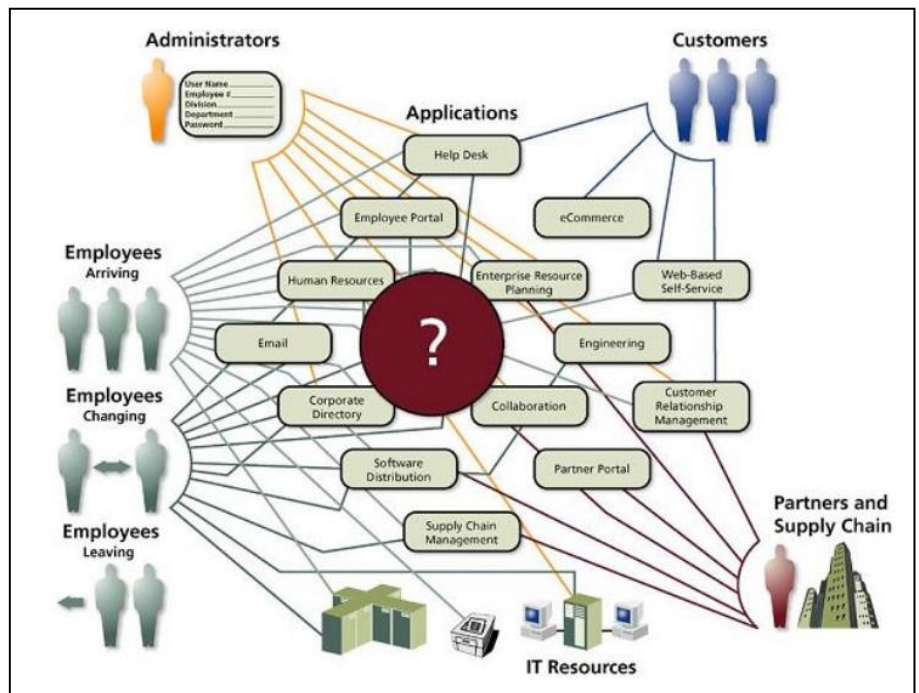


Figure 1: The typical enterprise: user information and access controls are fragmented and duplicated across multiple systems

This labyrinth of inefficient processes and overlapping systems, held together by the digital equivalent of "bailing wire and chewing gum," can have significant consequences for:

Cost Containment and Productivity

- New employees and contractors wait days to receive access to needed applications.
- Line managers, and IT and human resources staffs, devote endless hours to completing forms, entering user data, setting up accounts, and resetting passwords.

Security

- Users are granted access rights in violation of security policies.
- Departing employees, contractors, customers and business partners retain access to systems for long periods, and "orphaned" (invalid) user accounts proliferate.
- The organization can't meet audit requirements or comply with government regulations.

Customer Service and Supply Chain Integration

- Customer service and cross selling opportunities are impeded by incomplete views of customer data.
- Customer web initiatives and supply chain integration projects are hobbled because enterprises can't confidently expose IT systems and sensitive information to outside parties

Examples of Strategic Impact

The situation described above may sound like a technical subject of limited interest to business managers. However, it can have a strategic impact on profitability and competitiveness.

Listed below are examples of enterprises that were blocked in their ability to pursue strategic business initiatives because of deficiencies in their identity management systems:

An investment management firm...

was unable to provide competitive service to its best customers because it could not precisely control access to confidential account information.

A healthcare company...

faced the prospect of failing a security audit because it could not comply with federal privacy regulations.

An insurance and financial services firm...

was unable to cross sell products and maintain competitive customer service because it could not provide its agents with a unified view of customer activities.

A major media company...

was publicly embarrassed when an employee gained unauthorized access to sensitive corporate information.

A leading construction management company...

could not increase revenue at planned rates because it was unable to quickly set up and activate computer systems at local job sites

A well-known university...

could not compete for top students because it could not quickly and confidentially process course registration information.

On page 9 of this white paper we will return to these organizations and look at how they overcame these problems with Secure Identity Management solutions.

What is Secure Identity Management?

The term “Secure Identity Management”¹ has come into use to describe the convergence of a group of disciplines and technologies that have been evolving independently over several years in response to seemingly independent problems.

The disciplines include *user account management*, *security administration*, *content management*, and *provisioning*.

The technologies include *directories* and *metadirectories*, *access control* and *single sign-on products*, *provisioning systems*, *content management tools*, and *portals*.

Analysts are now recognizing that these should work together in solving the fundamental business problem of managing who has access to resources and under what circumstances.

If we view Secure Identity Management as the harnessing of these disciplines and technologies together for a common purpose, then we can define the term as:

Systems and processes that control who has access to information resources and what each person is entitled to do with them.

But behind this simple definition lies a collection of complex functions. Secure Identity Management systems and processes must:

- **Identify** people as legitimate users with specific access rights
- **Authenticate** the people by verifying that they are who they claim to be
- **Authorize** each person to access specific applications and perform specific functions
- **Manage** the creation of user accounts and the addition, change and deletion of access rights
- **Enforce and audit** the granting and revoking of rights according to security policies
- **Respond** quickly to changes in users, information systems, and the external environment

The first three functions can be loosely characterized as “run-time” activities that take place when employees, customers and business partners attempt to access information resources. The last three can be described as “process” functions that automate the process of creating and changing access rights over the life cycle of users.

In the next section of this white paper we will examine a framework that describes how these functions are provided by a variety of systems and processes.

¹ Roughly equivalent terms from different analysts and vendors include “Identity Management,” “Identity and Access Management,” “Network Identity,” and “Digital Identity.”

A Secure Identity Management Framework

ePresence’s Secure Identity Management framework is divided into three components, as shown in Figure 2. We will look briefly at the functions and technologies in each component.

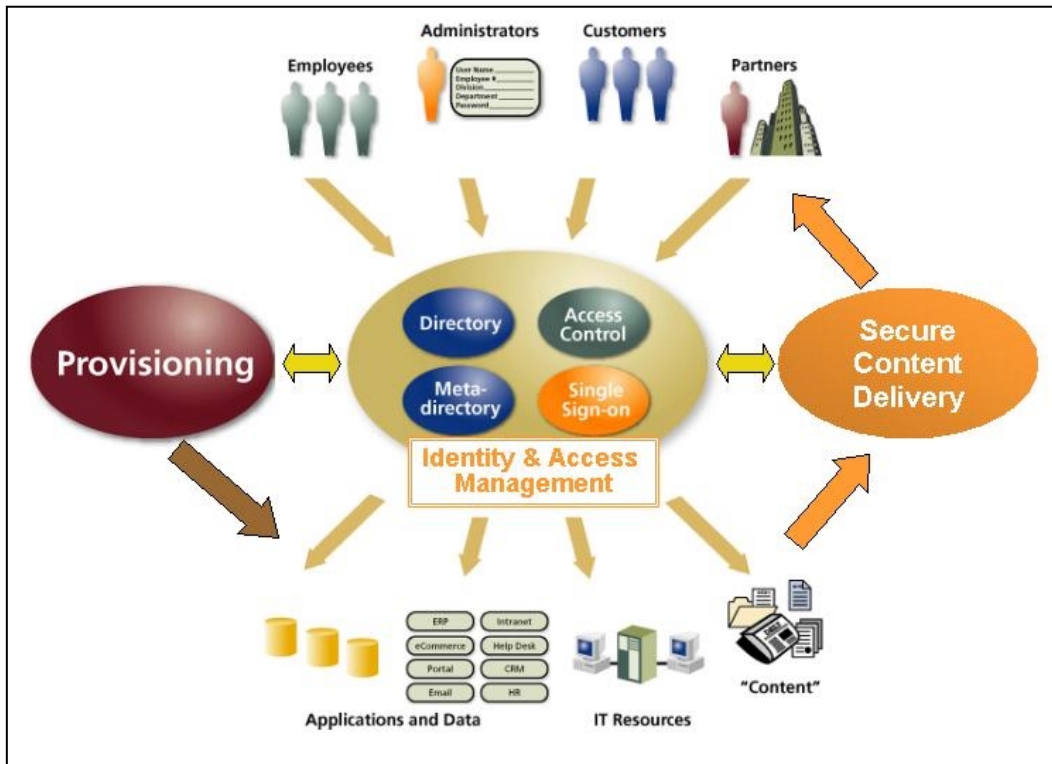


Figure 2: The major components of a Secure Identity Management framework

Identity and Access Management Services

Identity and Access Management services ensure that all users have access, on demand, to all of the information and systems for which they are authorized.

When a user logs on and requests access to a resource, Identity and Access Management services verify that:

- This person is an authorized user of the systems (“Identity”).
- This *is* the person he or she claims to be (“Authentication”).
- This person is authorized to use specific resources, and to perform certain functions with those resources; for example, reading, modifying or deleting records in a database (“Access Control,” or “Permissions”).

In essence, these services are the guard at the entrance of a highly secure building—holding the list of who can enter, checking identification, and escorting visitors to the locations they are cleared to enter—and performing these functions hundreds or thousands of times every minute.

The operational benefits of Identity and Access Management services include:

- A single, trusted source of identity information, so all applications and systems have a reliable, up-to-date view of users and their rights.
- Simplified administration, so administrators can add, change and remove users and permissions quickly and easily, in one place instead of many.
- Fine-grained access control, so administrators can control more precisely what resources users can access and what they can do with those resources.
- Fewer passwords and better password management, so users can access applications conveniently and help desk personnel can spend less time managing password problems.

Technologies

Directory and Metadirectory Services

An enterprise (or e-Business) *directory* is a repository of information about users and the resources they are authorized to use. Information stored in the directory might include name, address, groups or roles (“manager,” “contractor,” “Tier 1 distributor,” frequent buyer”), access rights to specific resources, policies on how those resources can be used, and data related to security (such as passwords and digital certificates). Directories may draw this information from a variety of “*systems of record*” such as human resources and accounting applications, email directories and web server registration databases.

Metadirectories create a virtual view of information stored in multiple directories. They can help present a unified view of users in organizations where user information is stored in multiple directories and user databases.

Password Synchronization and Single Sign-On (SSO) Products

Password synchronization packages automatically update a user’s password in multiple systems, so that he or she can use a single password to sign on to multiple applications.

Single sign-on products go further by allowing the user to sign on once, after which the single sign-on software logs onto other resources on behalf of the user. However, although “single sign-on” has become the standard name for this product category, it is a misnomer; a more practical (and still extremely valuable) goal is “reduced sign-on.”

Access Control Systems

Access control products authenticate users and control access to resources based on the permissions that have been granted to those users. To simplify administration, they typically apply permissions based on pre-defined roles (*Role-Based Access Control*, or “*RBAC*”) or on business rules. In this way policies can be set and applied for groups (e.g., “all sales managers have access to application X,” or “customers with a combined balance greater than \$10,000 can download document Y”). Some products provide *delegated administration* so that managers in a business unit can control user information. Most offer *self-service* capabilities so that end users can correct directory information or change passwords without involving the human resources department or the help desk.

Provisioning

Provisioning systems automate and streamline the processes for requesting, approving, adding, changing, and revoking user accounts and access rights for digital resources. These include email, telephone service, enterprise applications, HR applications, line-of-business applications, intranets and extranets, and help desk services. Automating these processes reduces costs and increases productivity dramatically. It also ensures that policies and procedures are followed consistently.

Provisioning systems can also automate processes for requesting and acquiring physical resources such as telephones, laptops, wireless devices, and building access cards.

“De-provisioning” is another key feature of provisioning systems. When an employee leaves, the provisioning system can quickly and systematically delete user accounts and revoke access rights.

The benefits of provisioning systems include:

- Faster “time-to-productivity,” because new employees and contractors gain fast access to the resources they need to do their work.
- Reduced costs, because automated workflows reduce the time business managers and IT personnel spend approving requests and creating user accounts.
- Improved security and auditability, because processes are applied consistently across all business units.
- Reduced exposure to information theft and sabotage, because rapid “de-provisioning” immediately removes access to resources when employees leave.
- Better asset management, because computers, cell phones, mobile devices and software licenses can be recovered promptly and recycled when employees leave.

Technologies

Workflow

Most provisioning systems incorporate *automated workflow* as a key technology to streamline the process of adding, changing and deleting user accounts and providing resources. Requests for resources are entered online, routed in a predetermined path to reviewers and approvers, and sent finally to the person or system that creates the user account or obtains the resource.

Some provisioning systems also include a *rules engine* that allows workflows to be varied according to a decision rule (e.g., sending high-value requests to a vice president for approval).

Reporting and auditing capabilities document who has changed policies and granted or revoked access rights to groups and individuals.

Connectors and Agents

Software “*connectors*” and “*agents*” link the provisioning system to the enterprise’s applications. For example, the provisioning system can communicate with the email server and automatically create an email user account, or a request for a laptop computer can automatically initiate a purchase order in the purchasing system.

A provisioning system works closely with Identity and Access Management services. It retrieves user and role information from directory services to know what resources and permissions to grant to each user. It also automates the process of adding users and updating user information in access control systems and directories.

Secure Content Delivery

Most organizations use one set of tools to control access to applications and databases, and another set of tools to control access to “content” (documents, spreadsheets, graphic images and other files). For example, the process of managing users for accounting systems may be wholly divorced from the process for managing users for the corporate intranet.

But by viewing content delivery as part of the overall Secure Identity Management framework, the enterprise can reduce duplication, enhance security, and improve productivity.

Content delivery systems can take advantage of the same Identity and Access Management services and provisioning systems that are used to control access to applications. User identity and role information can be used to target content to the people who can use it most—and away from people who should not see it. The access control and password management systems can simplify access to portals as well as to applications (or applications can be accessed *through* a portal). The provisioning system can automate the creation and revoking of access rights to web sites and portals.

Content delivery systems also add tremendous value in their own right by automating the process of targeting and publishing content, and by helping users find the content they need to do their jobs better.

The benefits of secure content delivery systems include:

- Improved user productivity, because users can find the information they need quickly.
- Enhanced security, because content can be concealed from inappropriate users.
- Reduced costs, because automated workflows decrease the time and effort required to develop, approve and publish content.
- Improved customer service, because personalization presents customers and business partners with exactly the content that they need to buy from or work with your company.

Technologies

Content Management Systems

A *content management* system automates the preparation, review, approval, and publishing of content to a web site or portal. A structured workflow carries materials from creator to editors, reviewers, and approvers, and on to the web site for publication. This reduces the delays and errors inherent in publishing processes. Further, the content management system gives creators and editors the chance to associate target audience information with a document. A memo, or manual, or product announcement could be targeted at “all employees,” or “design engineers” or “approved suppliers.”

Portals and Personalization

A *portal* is a web interface that gives employees, customers and partners access to the content and applications they need to perform work, or work with the enterprise. A “*personalization engine*” within the portal can match the target audience properties of a document with user information from directory services to determine exactly which individuals should have access to the document and how prominently it should be displayed.

Portals can also play a key role in other aspects of Secure Identity Management, for example allowing users to update personal information in self-service mode, set and reset passwords, and request access to applications through the provisioning system.

Results

The adoption of Secure Identity Management solutions is being led by:

- Enterprises driving to improve *operational efficiency*, who are finding that Secure Identity Management boosts the productivity of employees and reduces the costs of provisioning, user account management, and user support.
- Enterprises with a mandate to strengthen *security* and *privacy*, who have recognized that the capability to grant access rights correctly, and to terminate access immediately, is fundamental to protecting sensitive information.
- Enterprises engaged in *eCommerce*, *supply chain integration*, and *collaboration*, because Secure Identity Management enables the secure exchange of business information across organizations.

To see how Secure Identity Management solutions can help enterprises pursue strategic business initiatives more effectively, let us return to the examples that were cited earlier:

The investment management firm...

increased business with its best customers by implementing a directory-powered portal that provided access to account information precisely calibrated to each user (for example, primary account holder versus beneficiary of a trust).

The healthcare company...

substantially enhanced its ability to comply with government audit and privacy regulations by implementing an access control system that manages the registration of external users over the web and tracks their activity on the company's web site. Self-service password management capabilities also improved customer service and reduced help desk costs.

The insurance and financial services firm...

improved customer service and cross-selling by creating enterprise directory services that provide 30,000 employees and 250,000 agents with a unified view of customer account information. In the process, the firm also greatly increased the consistency and accuracy of data about employees, agents and customers, and shortened the time needed to deploy new applications.

The major media company...

plans to use a secure content delivery system to reduce its exposure to information theft by controlling access to confidential documents. The company also anticipates productivity gains from streamlining document management for legal, sales and customer service processes.

The leading construction management company...

was able to increase revenue aggressively by modernizing platforms and streamlining processes so that it could quickly set up and tear down computer networks at remote job sites.

The well-known university...

can compete better for top students because a provisioning system allows it to process over 30,000 student registrations smoothly in a two-week period at the beginning of each term.

Where Do You Start?

Secure Identity Management addresses many processes and systems, and clearly it is impossible to implement all of the components at once. Fortunately, there are many elements within the framework that can provide a rapid payback.

A few initial steps may be dictated by technical consideration. For example:

- Migrating to up-to-date **computing platforms** (operating systems, email and networking software, web servers) to create a stable infrastructure to support Secure Identity Management systems.
- Implementing enterprise **directory and metadirectory services** to create a trusted identity store containing information on user identities and roles, so that these can be used by access control, provisioning and other systems.

Beyond these initial prerequisites, choosing the most advantageous steps depends on the needs and priorities of the organization. The ePresence Secure Identity Management Continuum, shown in Figure 3, suggests one typical sequence of events.

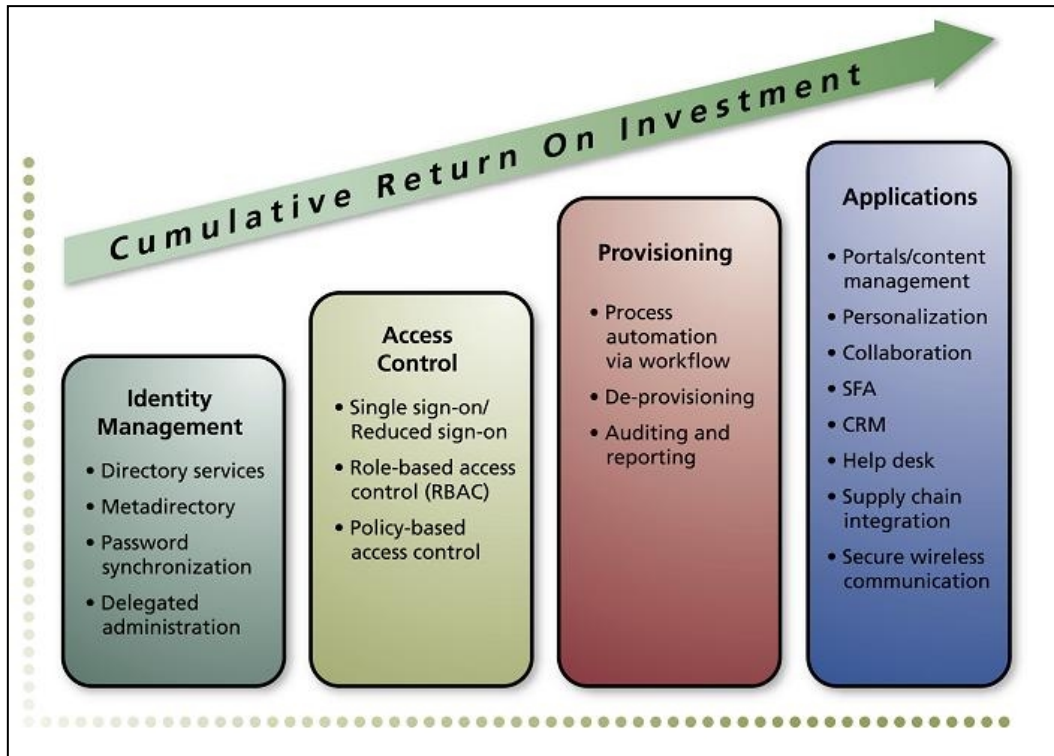


Figure 3: The ePresence Secure Identity Management Continuum

Note that an enterprise should always analyze its business drivers and existing technical environment before deciding on a course of action. This analysis will highlight the projects that provide the biggest initial “bang for the buck,” and will also help determine the criteria for selecting products.

ePresence—A Partner for Secure Identity Management

If you would like an experienced partner to help you begin enjoying the benefits of Secure Identity Management, ePresence is the perfect choice.

We help our clients understand how they can apply Secure Identity Management processes to improve their business and advance strategic initiatives. We help set priorities, create business justifications, evaluate products, and develop phased implementation plans. And we help design scalable, flexible architectures, install software, integrate and optimize systems, and train users and technical staff.

ePresence is the largest consulting and systems integration firm exclusively focused on the Secure Identity Management field, with nineteen years experience implementing Secure Identity Management solutions for Fortune 1000-class clients such as ChevronTexaco, Turner Construction, the Commonwealth of Massachusetts, and hundreds of others.

We have strategic alliances with industry-leading platform and technology vendors such as Microsoft, Sun, IBM, Netegrity, Critical Path, Access360, and Business Layers.

ePresence was recently recognized by IDC as “One of 20 services firms that matter.”

If you would like to learn about:

- A ***Secure Identity Management Discovery Service*** to assess your current identity management systems, evaluate opportunities to deploy Secure Identity Management solutions, and create a custom roadmap for moving ahead, or
- How we can help you deploy a specific Secure Identity Management solution such as ***enterprise directory services, metadirectories, access management, single sign-on, provisioning, or directory-powered portals***,

please contact us at 508.898.1000 or info@epresence.com, or visit us on the web at: www.epresence.com.