

# A Question of Identity (Management)

Identity Management has become a top priority for IT professionals.

By Larry Chaffin, Director of National Professional Services, SARCOM



The issue of Identity Management (IdM) in the enterprise is wide-ranging in scope and strategic in nature. It entails multiple components that are neither well-defined nor uniform across different organizations. And, as a subject that is both complex and vague, it can mean different things to different people.

What can we say about IdM, then, and why is it so important? In a real-world context, and from SARCOM's perspective, "Identity Management" is the umbrella term for the enterprise-wide mix of processes, policies and networked technologies for managing computer-user access, accounts, passwords and the provisioning of services.

## Why is IdM necessary?



**IdM is at the root of secure, safeguarded and trustworthy networked computing systems**

Why is IdM necessary? IdM is at the root of secure, safeguarded and trustworthy networked computing systems. Usually driven by a company's security policies and regulatory compliance efforts, IdM authenticates users and validates access to individual computers and networked systems (devices, folders, drives, databases, repositories, directories, etc.), as well as provisioned services and applications (e-mail, Internet, middleware, etc.).

IdM not only factors in user identities, it also holistically covers the identities of the devices, folders, drives, databases and other networked systems, services and applications. Consequently, IdM is a means for managing digital identities and tailoring the digital experience so that it is customized for each individual user, according to the user's profile and preferences, whether the interaction is for business, entertainment, discussion or shopping

Additionally, IdM has the flip-side effect of protecting confidential personal and business information from unauthorized users, both within the company and external to it. As such, it serves as a key vector in the world of electronic commerce and online transactions, including business collaboration through extranets.

Identity management also extends to a company's bricks-and-mortar infrastructure with respect to user access to entry points, equipment rooms and facilities in general.

Back in the world of digital identity management: Because of its implications for overall security in general, and information security in particular, any planning of an IdM initiative must be done by mapping it to the company's policies for security, trusted computing and privacy. This effort must span digital data, networked systems and human identities alike, including basic requirements and provisions for making changes to passwords, to cite just one example.

Being able to make changes to any part of the IdM solution quickly is important, considering the range and constantly evolving nature of malicious external and internal threats. These threats evolve and grow constantly, as computer worms, viruses, phishing attacks and identity thieves constantly try new ways to gain access to corporate data and personal information.

## Components and Considerations

Against that backdrop, what are the main components of an identity management system? What should you look for when selecting and deploying a solution?

As the research analysis firm Gartner said of IdM projects, “These initiatives are complex and expensive, so they require an approach that is both strategic and flexible.”

This point is especially pertinent because of the many products and solutions — and their widely varying quality and effectiveness — available for identity management. The point made by Gartner also underscores the importance of product interoperability and the preference for a standards-based solution; i.e., in accordance with Liberty Alliance specifications, Security Assertion Markup Language (SAML), or Web Services specifications.

Gartner makes another valid point, which is that “not every enterprise should implement all facets of the complete identity management solution, such as password reset, user provisioning, extranet access management, single sign-on, directory consolidation and role management.”

There simply may not be a need for one or more of those elements. Every identity management solution is modular in nature. Identity management solutions developed by SARCOM are customized to match the specific needs of each business customer. Each solution covers a complex mix of sophisticated processes and technologies — but each is tailored to suit the particular company for which SARCOM is implementing the solution.

The next step is to consider the underlying identity management architecture.

SARCOM’s identity management architecture model aggregates a sophisticated set of resources, including policies, networking equipment, digital certificates and encryption.

## Understanding the Architecture

The foundation of a typical identity management architecture (*outlined in Fig. 1, above*) is the **Company Business Policy** that sets certain standards by which the business needs to operate. This underlying business policy is defined by the company’s corporate governance board.

Working up from the foundation, or company business policy, the IT department establishes a **Domain Policy Template** that can be applied to departments and divisions across the enterprise. The next layer up is a **Policy Deployment Template** that defines how “domain standards” are applied to any section of the enterprise requiring a policy for identity management.

These domains are divisional, departmental, or virtual/physical locations designated as **Policy Enforcement Points (PEPs)**, which represent specific resources — everything from door-side badge readers to digital certificates providing access to sensitive network data.

The above graphic shows two departments — Accounting and Human Resources — which represent domains identified in the company business policy at the foundation of the identify management architecture.

From each domain, the graphic points to three examples of policies established for specific Policy Enforcement Points starting at the domains and spanning across the enterprise and its network.

In this example, both Accounting and Human Resources have three deployment policies driving what happens at the corresponding Policy Enforcement Points:

- **Data Policy Deployment** for digital certificates, firewalls, access control lists (ACLs) and encryption
- **Employee Policy Deployment** for ID badges, biometric scanning and pass codes
- **Guest Policy Deployment** for visitor identification, guidance and hours

This example provides merely a high-level overview of a basic identity management architecture framework that can be applied to any business model. Building and applying such a framework will safeguard the business’s employees and other assets, promote compliance with governmental regulations, enhance ROI on IT investments and demonstrate due diligence to protect against a liability action. When policies are in place and enforced, the company will operate efficiently and establish an environment for business growth.

To learn more about SARCOM’s services for identity management, contact Larry Chaffin, director of national professional services, at 614-854-1132 or [larry.chaffin@sarcom.com](mailto:larry.chaffin@sarcom.com).