

## WHITE PAPER

---

# Finding a Comprehensive Password Management Solution: The Initial Piece of the Identity and Access Management Puzzle

Sponsored by: CA

---

Sally Hudson

August 2007

## IDC OPINION

Increasing global regulatory compliance mandates, combined with budgetary and staffing constraints, continue to drive organizations to look for better ways to cost-effectively manage their IT security infrastructure. Identity and access management (IAM) products are a key component of a secure compliance platform to deal with the following issues:

- Password policies are a top concern within IT departments and are included as key IT control for compliance.
- Companies will implement IAM technology to centrally define and enforce a global password policy.
- Investments to automate user and access control can be leveraged across multiregulatory environments.
- Companies need to be proactive, not reactive, in developing, educating, and enforcing enterprisewide security policies and procedures.

## IN THIS WHITE PAPER

In this white paper, IDC outlines the issues surrounding user passwords and password management and examines how this technology often serves as a starting point for organizations looking to implement an IAM solution to increase security and achieve compliance. IDC has incorporated elements of the following categories into its research methodology for this document:

- Reported and observed trends and financial activity within the industry
- IDC's Software Census interviews (IDC interviews all significant market participants to determine product revenue, revenue demographics, pricing, and other relevant information.)
- Product briefings, press releases, vendor financial statements, and other publicly available information
- IDC's extensive demand-side research initiatives

## SITUATION OVERVIEW

IAM solutions exist to provide a centralized solution for enterprise accounts regardless of their physical/logical location. IAM serves to manage identities for mainframes, Web portals, databases, directories, and mobile environments while providing authentication and account provisioning/deprovisioning functions. This need has been compounded by the explosion of client devices and end-user (or end-use) devices found at the network edge. IDC calls this phenomenon "pervasive computing." Pervasive computing has had a considerable impact on the need to expand the security infrastructure. Subsequently, organizations have an urgent requirement to create a strong, secure, and flexible architecture capable of managing these rapidly multiplying user identities among the growing number of applications and services found within their corporate software catalogues.

The password represents the first and perhaps most essential piece of this puzzle. End-user passwords are still the dominant identification and authentication method in computing today. A user simply enters a character string, which is then submitted over the network and matched against a passwords database or an authentication software program. What could be easier? For many years, this was enough. However, the need to balance end-user convenience with effective security and password policies has become increasingly important in today's ever-expanding world of IT boundaries.

---

### **The Weakest Link: The End User**

It is well known that passwords are vulnerable to password-cracking tools, keystroke monitors, and network sniffing. Data shows that incidences of ID fraud and theft are on the rise. An Anti-Phishing Working Group report in 2006 revealed more than 360% growth in phishing sites from May 2005 to May 2006 and over 425% growth in password-stealing malicious code during the same time frame.

However, by far the greatest risks for compromising the integrity of a password are generated by the end users themselves. These threats are usually introduced to the enterprise by non-technical means.

It has long been acknowledged and lamented that people are indeed the weakest link in the ID/password security implementation process. This has been proven through various and often blatant demonstrations of lack of understanding of what is at stake (e.g., yellow Post-its with passwords found on user terminal screens, employees calling in and asking a non-IT professional to log in to their system to retrieve something, letting colleagues "borrow" a password when they have forgotten theirs); and the list goes on. Simple forgetfulness is perhaps the most common reason that passwords need to be reset. Prior to self-enabling password reset functions in password management systems, it was estimated that 50% of all help desk calls on a given day could be related to password resets. The following excerpt from an April 2006 *InfoWorld* article illustrates the dilemma:

Security should be everyone's job, from CTO to administrative assistant. It's surprising how few organizations recognize this. I think back to a time right after a fairly large network upgrade. All weekend, day and night, had been spent migrating a nightmare network.... Things hadn't gone quite as smoothly as we'd hoped, so instead of

finishing up on Sunday afternoon, we were still putting final tweaks in place on Monday morning. After we did our last test (making sure all local tape backups were working properly) it was about noon. (Most users by now had logged in, been informed that they needed to choose a new password in accordance with our medium-strong password guidelines, and had chosen a new password.) I stumbled bleary-eyed into the lunchroom for my umpteenth caffeine fix. ... it grabbed my attention from the corner of my eye. ... "Password List." Yes, every user's new password along with IT and even some specific switch passwords had been printed out by a well-meaning secretary and posted in the lunchroom. After they pried my hands from her throat, *she explained that she just figured it'd be easier to post them there than to answer all the phone calls when users inevitably forgot them.* So she went around and collected them (in my name), built her list, and posted it.

The following excerpt from a *Computerworld* article provides another, even more disturbing real-world example:

February 12, 2007 — In Lancaster, Pa., last week, the county coroner was brought to court in handcuffs. A grand jury indicted ... charging him with giving out his account name and password for a county Web site that contained confidential police 911 information. ... Names of accident victims and police informants, medical conditions, witness accounts, autopsy reports, and not-yet-substantiated accusations. The site was the access point for real-time data generated and used by firefighters, ambulance crews and other emergency responders.

And who did the coroner allegedly give his password to? Newspaper reporters. ... because he didn't want to be bothered with their phone calls asking for details about homicides, fatal accidents and suspicious deaths.

According to the *Computerworld* article, an IT staffer *eventually* checked Web site logs and discovered that the site was accessed 50 times over a two-week period from computers located at a newspaper office. This security breach was uncovered only after one reporter referenced information from the Web site in a news report and a competing newspaper called the county to find out why it didn't have access too. It was then, the article goes on to say, that "a police investigation began, logs were checked, passwords were changed, and the grand jury went to work."

Help desk involvement in simple password reset has been estimated over the years to cost anywhere from \$20 to \$250 per call, depending on the size of the organization and the number of software systems involved. Compounding the situation, the majority of large organizations require that users maintain more than one password to access many different systems. For example, in a medium-sized organization with 1,500 employees, the average annual cost for managing passwords can easily add up to \$375,000 or more. In addition to the obvious time and money factor associated with resets, as well as the administrative nightmares inherent in these situations, the real security dangers arise when frustrated users share (and even post!) passwords.

IT security professionals are keenly aware that a lack of password management and access control measures can lead to disasters. When organizations fail to properly manage user passwords and identities, password rules and recycling can lead to password-related vulnerabilities. Over the years, many well-publicized IT security breaches have been related to administrative oversights in removing IDs and access privileges of former employees or users. While this leads into the importance of provisioning and deprovisioning practices and products, in the beginning it starts with the password. Strong passwords and well-defined password policies are essential for overall system security and well-being.

---

## **Password Management: A Cornerstone of the Corporate Identity Foundation**

The ability to effectively deploy enterprise password management solutions has already had a major impact in many enterprises and organizations. When selecting a password management solution, IT professionals and business administrators should have the following features and functions on their short list of requirements to allow for self-service and ease of use:

- Self-registration, which enables a user to specify a password when registering at corporate Web sites
- The ability for a user to modify or change a password without involving the IT help desk or other personnel
- The ability for a user to readily retrieve a forgotten password after verification of identity

From a security and password policy perspective, password expiration parameters are important. They allow an administrator to set a maximum number of log-in failures and define inactive password policies and the time period in which the password expires. Expirations can also be set for time variables, which force the user to reset current passwords.

Password composition rules are also important. They allow for the creation of strong passwords by defining their composition in terms of minimum and maximum characters and types of characters and by incorporating the use of uppercase and lowercase letters as well as the use of blank space.

Password synchronization capabilities are critical because they reduce the number of passwords a user has to remember when accessing various applications on the corporate network. The synchronization function allows users to have a single password with which to access all of their provisioning accounts. Additionally, reverse/bidirectional synchronization can be used to verify passwords between assigned target systems and applications utilizing the administration tool's password policies. These functions allow the system to automatically verify and reestablish access based on preestablished policies.

IDC views password management as a cornerstone of a comprehensive IAM solution. A total IAM foundation also includes secure enterprise single sign-on (ESSO) and provisioning solutions. ESSO (or host SSO) enables users to log in to internal applications, databases, and other corporate systems with just one identity. ESSO solutions enforce password policies and eliminate the need for employees to remember multiple passwords. In addition to providing a high level of password security and simplifying the password management process for employees, a well-developed system also relieves the IT staff of additional burdens — freeing them to work on more urgent system matters. End users do not have to remember different credentials for different applications.

User provisioning automates the process of granting access rights, automates the process of changing those rights, and in some cases, audits the appearance of inappropriate rights in a user's profile. By automating time- and cost-sensitive manual procedures, user provisioning can sharply reduce the costs of granting new employees, customers, partners, and suppliers the necessary access.

ESSO and user provisioning are part of the larger world of IAM. IDC defines IAM as a comprehensive set of solutions used to identify users in a system (employees, customers, contractors, and so on) and control their access to resources within that system by associating user rights and restrictions with the established identity. ESSO is an important consideration for the growing enterprise. Having an identity management solution that enables integration with SSO solutions ensures that enterprise long-term imperatives can be met without having to "sunset" (retire) a limited password management solution. IAM solutions can also evolve to include federated identity (or FSSO), which is the ability to share a user's log-in and authentication data across different Web sites and applications, both internal and external to the organization, using secure, standards-based protocols. The user is able to sign on to multiple Web sites regardless of the provider or identity domain, and organizations are able to separate employees from external parties to better meet compliance regulations.

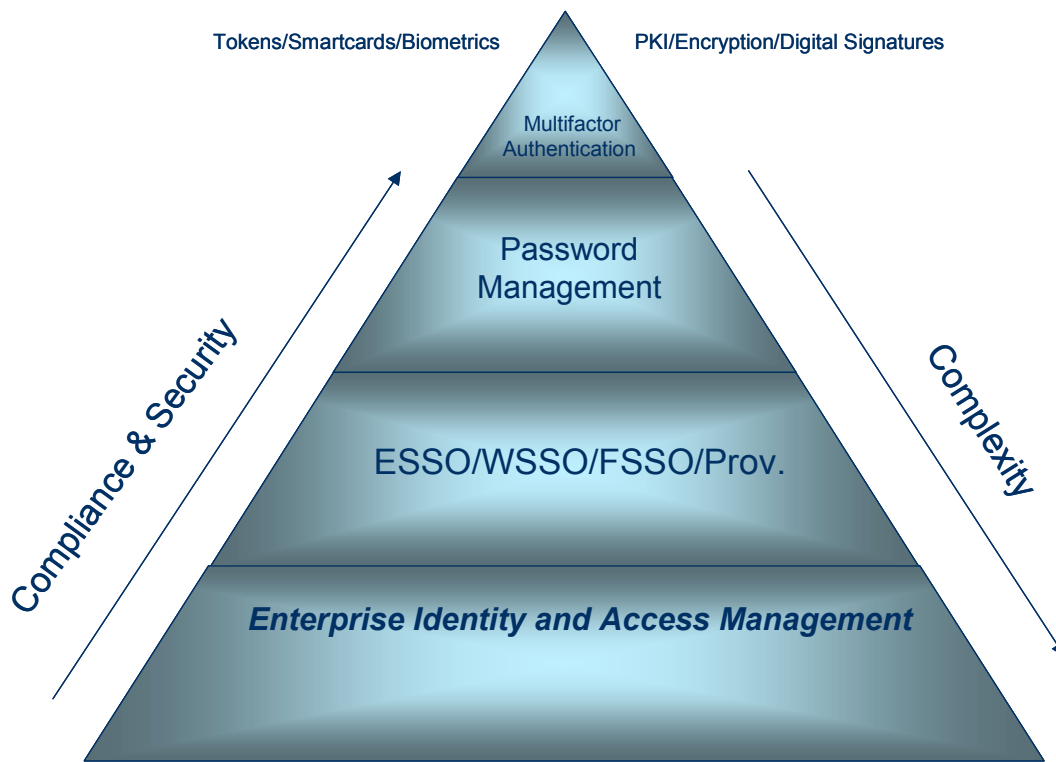
### ***Regulatory Compliance Concerns***

Compliance and security are the primary market drivers for IAM software and IAM products. IDC research shows that they accounted for 70% of all IAM purchases in 2005 and 2006. It is evident that government and industry regulations are placing unprecedented pressure on corporations to secure access to information and applications — not just with employees but also with customers, partners, and contractors. Organizations addressing compliance issues surrounding Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLB), the Health Insurance Portability and Accountability Act (HIPAA), and other federal regulations are increasingly looking toward IAM solutions to help them comply. These pressures are felt worldwide as international regulations such as Basel II, the Personal Information Protection Act (PIPA) in Japan, AIPA in Italy, FSA in the United Kingdom, and EUPA in Europe, and others are forcing regulatory compliance to become a global C-level issue. Each of these regulations can carry criminal penalties and/or civil penalties.

To meet both government- and industry-driven regulatory requirements, most companies employ a variety of IAM technologies, including provisioning, password management, privileged password management, digital signatures, secure single sign-on, audit and reporting, and two-factor and multifactor authentication mechanisms. Increasing global regulatory compliance mandates combined with budgetary and staffing constraints will continue to drive organizations to look for better ways to cost-effectively manage their security infrastructure. Figure 1 shows key technologies as they relate to the enterprise need for better security.

**FIGURE 1**

The Password Management Hierarchy



Source: IDC, 2007

While reducing cost and help desk calls is often the original motivation for companies to purchase password management and synchronization tools, these tools usually become the first step to implementing a comprehensive, enterprisewide identity management framework. Enterprise-class identity management software allows corporations to build on top of password management by setting access policies and establishing rights and privileges for both employees and other users of corporate-owned applications. Enterprise IAM software consolidates user identities and creates roles and access rights, and it stores and manages this information in a central repository that interacts with an ever-changing landscape of corporate applications, business and security policies, and increasingly, Web-based services.

## **The CA Approach to Identity and Password Management**

IAM is a critical success factor for today's enterprise. Total market revenue in IAM reached almost \$3 billion in 2006, and IDC forecasts it will reach over \$4.9 billion by 2011 (exclusive of IAM services).

CA has consistently been a market leader in IAM, and this technology set is a core component of CA's security management and enterprise IT management (EITM) strategies. The company offers a full suite of IAM products from Web to mainframe that includes CA SiteMinder® Web Access Manager (WAM) for WSSO/FSSO, CA Single Sign-On (CA SSO) for ESSO, CA Access Control, CA Embedded Entitlements Manager, CA TransactionMinder®, CA Top Secret®, and CA ACF2™. CA also offers auditing and reporting capabilities via its CA Security Command Center application.

In the area of password management, CA has a strong market offering in its CA Identity Manager, which provides password management, provisioning, identity administration, and virtualization for customers looking to create an automated and secure identity foundation for their enterprise. CA's solution allows organizations to centrally manage and leverage identities both internal and external to the company. This includes full-time and part-time employees, contractors, partners, assets, IT resources, applications, and roles. The standards-based software is designed to support and integrate with existing systems across the customer's organization.

Given that user and provisioning information is among the most sensitive data within an enterprise, CA Identity Manager has been architected to provide strong security via secure authentication, authorization, and encryption capabilities. CA SSO is also integrated with CA Identity Manager to manage the user's account, including setting the SSO password and setting/resetting the target system passwords. CA SiteMinder WAM shares a Policy Server with CA Identity Manager to provide two-way integration. The user roles defined in CA Identity Manager are automatically available for role-based access control enforcement via CA SiteMinder WAM.

While a comprehensive IAM enterprise infrastructure can take an organization from soup to nuts for secure ID management and compliance, most corporate entities start with the need for secure password management to solve their most immediate and glaring problems. IDC believes that CA Identity Manager provides a high level of security and administrative functionality with its password management and synchronization. Native integration allows CA Identity Manager to create and store passwords within the password "vault" of CA SSO. The Password Manager provides all of the criteria mentioned earlier, including user self-reset, reverse synchronization, strong password policy creation, and self-service registration and management. The password management component of CA Identity Manager also provides Microsoft Windows GINA support.

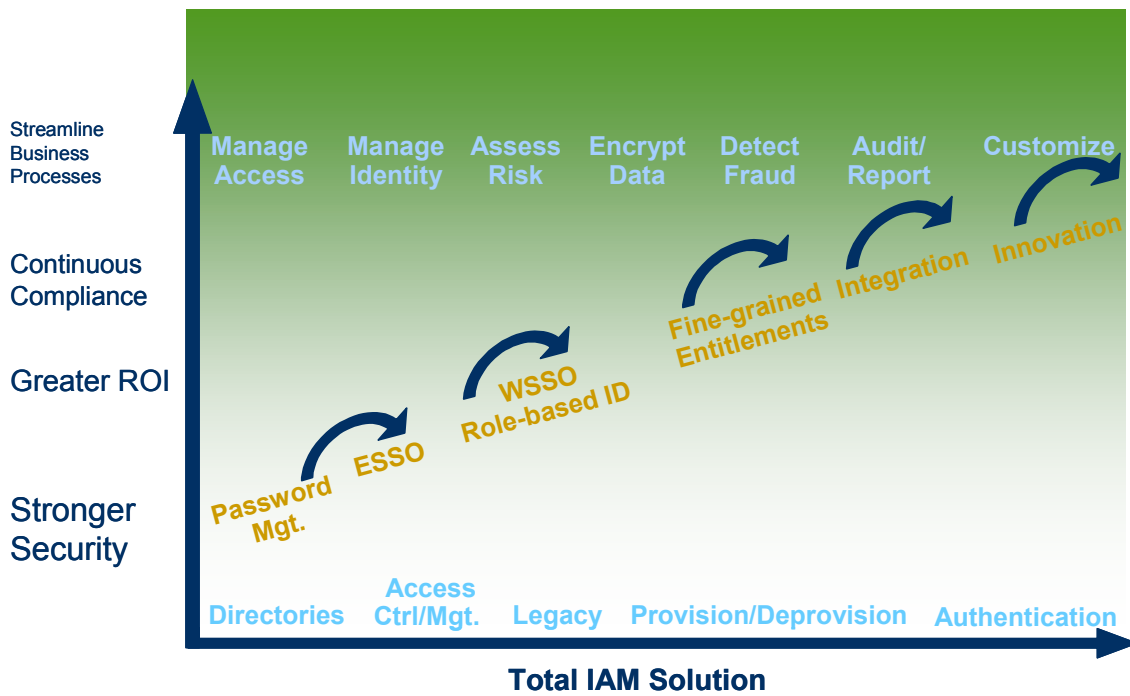
Another important capability of CA Identity Manager is the vendor's out-of-the-box integration via connector technology. These prebuilt connectors allow customers to significantly decrease the time to value when implementing IAM by using native application interfaces to integrate with ERP systems, groupware, hosts/servers, authentication servers, databases, and standards such as LDAP and ODBC. Not

surprisingly, mainframe integration is an area of strength here for CA, and connectors are available for IBM RACF, CA ACF2, and CA Top Secret. A Connector Xpress is available to accommodate customers' homegrown applications.

All of these components are necessary and integral to creating a strong, flexible, and manageable IAM foundation within the enterprise that is capable of reducing complexities and overall costs for IT professionals while enhancing security and compliance functionality. Only when these needs have been met can the enterprise leverage these advantages for innovation in business process and business process management (see Figure 2).

**FIGURE 2**

Key Stages of Enterprise IAM



Source: IDC, 2007

## **FUTURE OUTLOOK**

Compliance mandates as well as budgetary and staffing constraints will continue to drive organizations to look for better ways to cost-effectively manage their security infrastructure.

IDC's *Worldwide Security Products and Services 2007 Top 10 Predictions* (IDC #204678, December 2006) noted that we are entering a time in which security will be integrated into the fabric of the IT infrastructure. There are many reasons for this trend. Chief among them are the following:

- ☒ Looming integration issues
- ☒ Continually growing importance of IT within business operations
- ☒ Rising value of transmitted and stored data
- ☒ Increasing sophistication of attackers
- ☒ Government and industry regulation

Many of these issues can be addressed by the deployment of IAM technologies. Further, security is becoming a value-add — not just a necessary evil or the purview of the paranoid — to many systems. Companies now understand that systems, storage, networks, and applications need inherent security. Customers demand security, but they want transparent integration with IT infrastructures so that it is effective and convenient.

## **CHALLENGES/OPPORTUNITIES**

Security and systems management issues must come together to solve client situations in areas such as identity management, risk management, and application consolidation. CA must emphasize and showcase its ability to enhance productivity, reduce risk, and lower total cost of ownership by linking prospects' business problems with its security, compliance, and system management solutions. A consultative approach to client problems is often necessary when implementing a compliance-driven IAM architecture within an organization.

CA must continue to constantly refine, customize, and carefully articulate its marketing messages. When developing go-to-market strategies, the company is making progress in identifying the different nuances, buying behaviors, and security requirements of small, medium-sized, and large organizations, in addition to the various industries in which they operate. CA realizes that each segment and industry carries its own values and measurements for risk and return on investment, and the company should continue to develop and package solutions accordingly.

## CONCLUSION

The expansion of the enterprise workplace has greatly increased risk on a variety of fronts, and IT organizations are trying to manage this new environment. This effort will eventually require more usage of security management, IAM, and secure and content management technologies.

Furthermore, IT security personnel are in short supply. With a limited supply of trained security personnel, easier solutions are required. This need will drive the purchases of security solutions that are easy to use, reduce the need for trained security personnel, and add value to other IT solutions.

IDC believes CA is committed to continually refining, enhancing, and expanding its IAM suite to be SOA ready and integrating it with governance and compliance solutions.

## APPENDIX

---

### Definitions of IAM Technologies

**Web single sign-on (WSSO)** software enables companies to administer and consistently enforce user access to Web applications and provides SSO services to users. WSSO provides Web application security and identity management to employees, customers, partners, and contractors. Federated identity (or FSSO) technologies are derived from this market as well. FSSO is the ability to share a user's log-in and authentication data across different Web sites and applications, both internal and external to the organization, using secure, standards-based protocols. The user is able to sign on to multiple Web sites regardless of the provider or identity domain, and organizations are able to separate employees from external parties to better meet compliance regulations.

**Enterprise single sign-on (ESSO)** enables users to log in to internal applications, databases, and other corporate systems with just one identity. ESSO (sometimes known as host SSO) enforces password policies and eliminates the need for employees to remember multiple passwords. ESSO is a core component of a successful enterprise IAM architecture. A strong ESSO platform should provide a standards-based, secure approach to systems sign-on by eliminating the need for multiple passwords and allowing customers to leverage their IT existing investments while further expanding their identity management infrastructure.

**User provisioning** automates the process of granting access rights, automates the process of changing those rights, and in some cases, audits the appearance of inappropriate rights in a user's profile. By automating time- and cost-sensitive manual procedures, user provisioning can sharply reduce the costs of granting new employees, customers, partners, and suppliers the necessary access.

**Advanced authentication** includes software tokens and software designed to support hardware authentication solutions (tokens, smart cards, biometrics). It also covers many services associated with the creation, dissemination, validation, and protection of digital certificates. A portion of this market also includes public key infrastructure (PKI) technologies, which are designed to enable users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The PKI provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.

**Legacy authorization** includes mainframe access control used primarily on large computers, such as servers and mainframes, and very rarely on personal workstations. To do this, the software identifies and authenticates a user, determines the resources to which the user is authorized, and logs and reports attempts by unauthorized users to get access to protected resources. Typically, an IT administrator chooses which resources to protect and which users need access to them. The program can log any unauthorized access attempts either to the system or to a protected file and can notify the administrator with a report. This software, still widely in use today, had its origins in the 1970s.

**Hardware tokens** include traditional authentication tokens, which are small hardware devices that allow users to authenticate themselves to the token authentication server (TAS) using either one-time passwords (OTPs) or challenge/reply methods. These tokens can come in multiple form factors and do not require additional hardware. OTPs and challenge/reply tokens are simple to use and provide a robust authentication method. IDC also includes USB authentication tokens and software licensing authentication tokens (SLATs) in this segment.

---

## Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2007 IDC. Reproduction without written permission is completely forbidden.