

LARSTAN'S
**THE BLACK
BOOK ON**

**GOVERNMENT
SECURITY**

Unlocking the Doors to Identity
Management

**DR. ALASTAIR MACWILLSON
AND ERIC STANGE**

[6]

UNLOCKING THE DOORS TO IDENTITY MANAGEMENT

To determine the identity of those seeking access beyond the IT perimeter, governments must contend with the enormous complexity inherent in identifying individuals. To make the right decisions, managers must match identity to dispersed but relevant information – while at the same time, protecting privacy. Here, we discuss the best identity and access management methods, now and into the foreseeable future.

**“SCIENCE IS NOTHING BUT
THE FINDING OF ANALOGY,
IDENTITY, IN THE MOST
REMOTE PARTS.”**

— Ralph Waldo Emerson

by **DR. ALASTAIR
MACWILLSON AND
ERIC STANGE**

A knock at the door, followed by a response of “Who’s there?” This most basic question of identity is older than the tale of Little Red Riding Hood. But with new virtual doors opening online, accompanied by a growing threat from sophisticated

MANAGING I.T. COMPLEXITY IS THE BIGGEST SECURITY CHALLENGE FACING GOVERNMENT I.T. PROFESSIONALS TODAY. REGULATIONS ARE FORCING GOVERNMENTS TO ADOPT A MORE STRUCTURED APPROACH TO INFORMATION SECURITY.

and deadly terrorists, the answer has become more critical, complex and costly. Ruthless cyberwolves lurk everywhere.

These knock-at-the-door encounters occur across federal, state and local governments. At the border, international travellers “knock,” and a federal customs and border protection officer must quickly determine whether that traveller is who he or she claims to be, and whether the person’s intent is tourism or violence. At government offices at all levels, applicants “knock” to request benefits (payments, licences, privileges), and busy case-workers must determine whether to grant them. Security guards (human and electronic) scrutinize credentials to determine whether to admit people to secure areas. Millions of times daily, electronic petitioners knock at the door of IT security protections of systems and documents.

Although the nature of each of these environments is quite different, the underlying concepts and capabilities required to succeed are similar. To determine who is knocking at the IT perimeter, governments must meet key security and access management goals, such as:

- Improved Security — better protection from physical, electronic and financial threats
 - Improved Service — better and faster provision of benefits (access, privileges, payments, etc.) for legitimate petitioners
 - Improved Privacy Protection — stronger safeguards of personal information
 - Reduced costs — integrated solutions that cost less than previous and less effective approaches
-

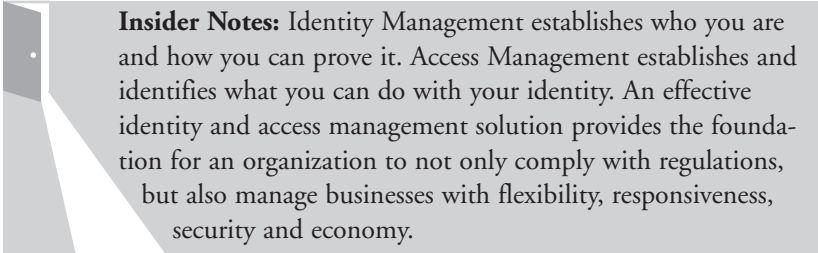
To accomplish these goals, governments must effectively manage the complexity inherent in identifying individuals, matching the identity to relevant information and making decisions, all while complying with appropriate regulations and judiciously safeguarding privacy.

Identity and Access Management (IAM) is the set of processes, people and technologies that control access to resources in the enterprise. Identity Management establishes who you are and how you can prove it. Access Management establishes and identifies what you can do with your identity. An effective identity and access management solution provides the foundation for an organization to not only comply with regulations, but also manage businesses with flexibility, responsiveness, security and economy.

MANAGING COMPLEXITY

Managing IT complexity is the biggest security challenge facing government IT professionals today. Regulations are forcing governments to adopt a more structured approach to information security and at the same time making departments more cautious in their use of security tools, products and services. Simple tools, such as a photo ID or a password, remain preferred credentials and access methods, despite the increased threat. While governments inform employees of privacy and behavior standards, the security of citizen data is often not as rigorous as it should be.

Identity schemes today are complex and fragmented, either by accident or design, with separate schemes implemented by government functions. The reason for this is that governments drive their security decisions from national priorities, but implement them at the agency/entity level. As the public sector, and the commercial sector for that matter, sifts through the

A graphic element consisting of a grey trapezoidal shape with a white dot on the left side, containing the text of the Insider Notes.

Insider Notes: Identity Management establishes who you are and how you can prove it. Access Management establishes and identifies what you can do with your identity. An effective identity and access management solution provides the foundation for an organization to not only comply with regulations, but also manage businesses with flexibility, responsiveness, security and economy.

complex area of information security, new technologies and increasing demands are moving at a pace that makes it difficult to keep up.

For example, eGovernment opens up “online 24x7 self-service,” without effective identity protection. Moreover, to deliver effective eGovernment services, there is a need for horizontal and vertical government integration, between departments, and among federal, state or local levels, which requires some kind of identity interoperability. There also is a continued push for high performance in governments, with expectations to provide better outcomes for less cost through increased efficiency and effectiveness.

The threat of terrorism and organized crime also drives the need for all government agencies, national, state, and local, to review their own technologies, policies and procedures. At the same time, it has exposed major deficiencies in current practices. Among other forms of crime, identity theft is experiencing exponential growth.

Citizens fundamentally expect their governments to protect them while simultaneously being protected from governments. If governments and individual departments are to fulfill this expectation, they must review existing approaches to identity and access management. They must create a future where the right people have access to the right information and privileges, as conveniently and quickly as possible, while inappropriate access is denied. In this environment, the significance and use of bulky, inconvenient credentials can disappear and be replaced by the person's innate ability to identify him or herself with their biometric identifiers. Once the government (or system) determines conclusively the identity of the individual, rapid information sharing is possible.

To achieve this vision, governments must be able to:

- Establish an identity at first contact that is based on firm truth and credentials, which assure that this person exists and is matched to this identity
 - Accurately verify the identity at each encounter to prove that the person is, in fact, the person he claims to be
 - Link the identity information to other relevant information, such as program eligibility, security clearance, citizenship, etc.
-


- Support decision making, by either presenting consolidated information to decision makers (e.g., at the border) or making the decision automatically (e.g., opening the lock)
- Protect the privacy of the individual, by securing it from inappropriate access, as well as facilitating legitimate review and corrections

DEFINING IDENTITY AND ACCESS MANAGEMENT

Data protection and security puts locks on systems. IAM provides the keys for those locks to individuals who need them to enter the right doors. Imagining a business or government using a different key for every single person for every single door, all managed by a different person in a different way, describes the state of identity and access management in today's computing environment.

IAM solutions require a technology implementation. However, this is only a part of the solution. Understanding the transformational nature of the processes and aligning the solution with the people in the organization is critical to the success of an IAM solution. These solutions transform the existing business processes that support the management of identities in the environment. Where possible, manual processes are automated and IT processes are simplified or distributed. Organizational change management and training are also critical components of an IAM solution. In addition, the definition of the organizational structure into a role and permissions model can provide significant value through automation of user access.

The scope and complexity of Identity and Asset Management challenges, and the associated holistic solutions, are vast. Our discussion will therefore focus on the core issues associated with technical components of these



Insider IAM solutions require a technology implementation. However, this is only a part of the solution. Understanding the transformational nature of the processes and aligning the solution with the people in the organization is critical to the success of an IAM solution. These solutions transform the existing business processes that support the management of identities in the environment.

solutions. The key technologies of IAM include Identity Management, Access Control, Provisioning and Identity & Policy Repositories. Integrated together, these technologies provide a platform to support an end-to-end IAM solution.

DELIVERING VALUE TO GOVERNMENT

It is often assumed that the adoption of IAM is largely driven by regulatory pressures on government agencies to sort out the inconsistencies within their internal processes, and within their management of individual identity data. However, for more visionary agencies, the real benefit IAM offers is the ability to interconnect, interoperate and to actually address some of their pressing business requirements. The real driver behind the rising attraction of IAM is the pressure on government to perform several new tasks. These include a plethora of eBorders type work, an avalanche of new demands for inter operative systems and the general desire to allow people access to systems and services to which they never had access before.

At its simplest, it can be argued that government must perform three fundamental roles:

- ❶ Protect national interests
- ❷ Serve citizens
- ❸ Protect costs/equipment (assets)

If we follow this approach, it becomes easy to illustrate how identity and access management policies, processes and technologies can combine to deliver previously unheard of controls for government, as well as improved performance at reduced cost.

The value proposition of IAM in government includes:

- Increasing security
 - Allowing for innovation and interaction among employees, partners, customers, supply chain managers, etc.
 - Facilitating regulatory compliance
 - Providing a comprehensive audit capability
 - Improving productivity and internal service levels
 - Reducing administrative and development costs
-

FIGURE 1

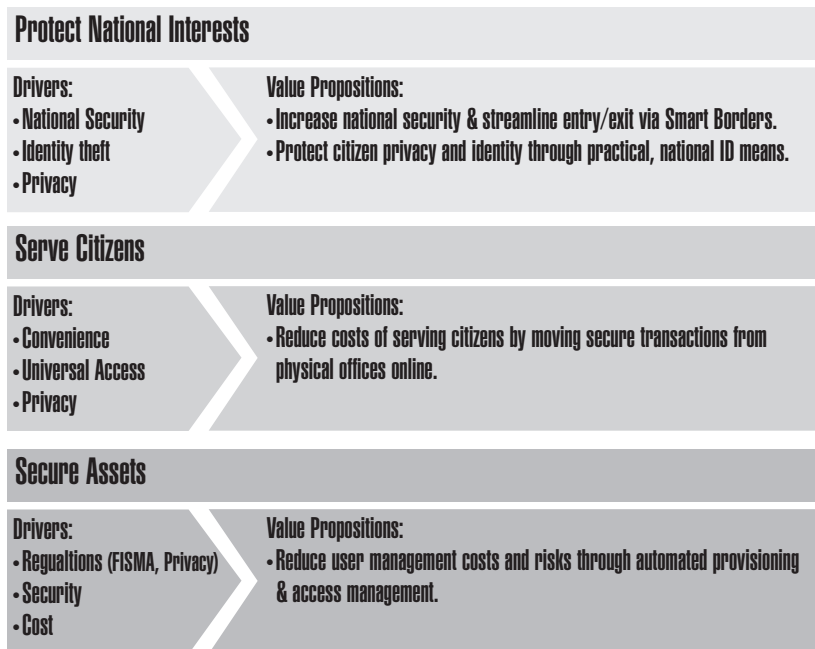


Figure 1 illustrates the drivers and value propositions for each of these government priorities.

Another way to consider the value of IAM is to assess benefits across three main areas: Business, Function and Security.

BUSINESS VALUE

The business value of IAM centers on:

- More effective management of user access based on business need
- Improved service to users

The big issue for government organizations, in fact for any organization going down the IAM route, is how to maintain control of their users and their users' access to organization resources. That is what IAM is all about. An important business driver is the fact that user administration processes are extremely costly. Features such as call centers and help desk volumes

(where users call for password resets because they can't get into an application) can be incredibly expensive in a big organization. Reducing cost center volumes clearly increases user productivity.

A clear benefit of IAM is that it sorts out the problem of being able to audit who does what. It links user identity with their access to different application systems, which simplifies the tracking of exactly what users are doing and ensuring that they are authorized to do it. This is very important from a government perspective and also addresses a second driver, regulatory compliance, which is linked to the ability to provide an audit trail and demonstrate that employees are properly segregated.

Another important business benefit is the potential for dramatic improvement in the quality of service in providing access to systems and resetting passwords. This is linked with improving performance. The issue addressed is the existence of multiple identities for single individuals, a problem that plagues most organizations. Historically, multiple identities have emerged because of the lack of clear identity strategies.

Government is particularly troubled by this dilemma. Agencies might have multiple separate identities for each individual, which costs much more to manage. The intention of IAM is to reduce this identity miasma to one single, ubiquitous identity for each individual that can be used across all systems.

FUNCTIONAL VALUE

Functionally, IAM improves:

- Access administration
- Access ownership
- Access oversight and control

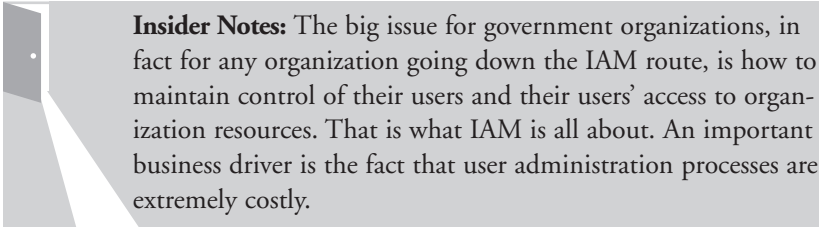
A key functional benefit of IAM is administration, or delegation, of the security administration. For example, when someone joins our company, Accenture, they get recorded onto the personnel system. If IAM is not in place, then somebody has to identify what systems that person needs to access and go through a process of getting that person enrolled on those systems with the right circumstances.

With IAM, people still need to approve the hire, but it is all done as part of a workflow of the provisioning aspect of IAM. An individual joins Accenture; he gets enrolled on the HR system, which triggers emails to that individual's boss or bosses. These managers, in turn, interact and assert that he is a consultant who needs access to, say, 12 systems — do you give approval for that? It's a “click-on-a-box” type of approval, but it is proper approval. Delegation is all about getting the right approvals.

The other benefit of delegation, which is quite important, is that instead of going through a central administrator, these approvals can be pushed out to the business units or business owners that need to get their staff access. Not only are the approvals pushed out, but the administration itself is delegated out to the business units, rather than remaining an IT function. That is an important point, because it means that the process is much more accurate. It needs to go through fewer interpretations, with fewer people involved, reducing the likelihood of errors.

In addition, the people involved are functionally much closer and can give direct authority far quicker than a central administrator. This is a significant change in the way people do things. It pushes the user administration away from the classic IT organizational function and into the business functions. All businesses like that, but especially government, where different departments want to control their own users in a way that is consistent with standards.

Another key functional benefit is the ability to provide and maintain centralized control over system access. A company can centrally manage all policies that govern new hires, security, people changing roles or getting promoted and people retiring or terminating employment. The nice thing

A graphic for 'Insider Notes' featuring a grey background with a white, stylized door or panel on the left side. The text is positioned to the right of this graphic.

Insider Notes: The big issue for government organizations, in fact for any organization going down the IAM route, is how to maintain control of their users and their users' access to organization resources. That is what IAM is all about. An important business driver is the fact that user administration processes are extremely costly.

IMPROVING SECURITY IS AT THE CORE OF IAM. IF IAM DOESN'T IMPROVE SECURITY, THERE IS NO POINT IN PURSUING IT, REGARDLESS OF THE FUNCTIONAL DRIVERS.

about IAM is that these policies can be implemented electronically, or be represented electronically in the provisioning system. For example, if a policy says that somebody that is leaving the firm must get revoked on all of the systems within 48 hours, the workflow can be set up to make sure that it gets done in 48 hours. Emails and messages are provided to the people that have to authorize it, making them aware of the urgency.

Overall IAM provides fast track access. It gets people to access certain applications in the fastest possible way without any complexity. It also introduces considerable simplicity into their current activities. These clearly are the most attractive benefits for people considering the implementation of IAM.

SECURITY VALUE

The key security value of IAM is achieved through improved:

- Password policies
- Access revocation capability
- Process consistency

Improving security is at the core of IAM. If IAM doesn't improve security, there is no point in pursuing it, regardless of the functional drivers. There are several types of security benefits that would accrue to government. The first is the enforcement of password policies. These policies include minimum password lengths, mix of characters, frequency of change rules (passwords have to be changed every 30 days) and specific characteristics (they have to be randomly generated). Many government departments have encryption systems, which require very strict, stringent passwords. IAM automates this potentially painful process.

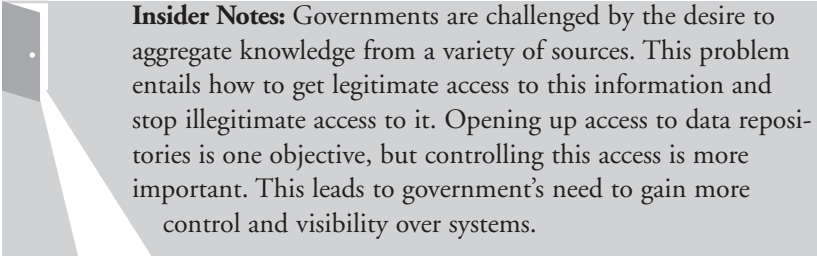
Another security benefit is being able to disable user access and privileges instantly, so when somebody leaves the company they can be easily deleted

by the fastest possible means. The third security benefit is the ability to manage the identities or the user account throughout its entire life cycle.

IAM also can help overcome the lack of a consistent security framework, especially in government agencies. If an IAM system is installed across multiple agencies, user administration and user processes could be applied consistently in accordance with policy and irrespective of the underlying systems, networks and approaches. It can function as the glue that sits across domains, providing a level of consistency. This is why it's regarded as an integrator between organizations.

It's no surprise that commercial mergers and acquisitions drive a good deal of IAM work. When two banks come together, chances are they use different technologies and systems, and adhere to completely different technology approaches. The only way to glue them together is either by making significant changes to one part or the other, or installing some common processes and systems that allow them to run in a singular manner. Also beneficial is the ability to enforce processes that ensure that people perform functions as specified within stated policies. This encompasses actions like minimum user password links or authorizations to certain systems.

IAM supports important government initiatives. Because one intention of IAM is reduced paperwork, it buttresses the U.S. Government Paper Elimination Act (GPEA). IAM also enables segregation of duties and auditing, supporting the Federal Information Security Management Act (FISMA), which is all about the proper segregation of duties, as well as reporting an audit trail of user activities and controlling their access.

A graphic for 'Insider Notes' featuring a grey background with a white geometric shape on the left side that resembles a stylized door or a folded page. The text is positioned to the right of this shape.

Insider Notes: Governments are challenged by the desire to aggregate knowledge from a variety of sources. This problem entails how to get legitimate access to this information and stop illegitimate access to it. Opening up access to data repositories is one objective, but controlling this access is more important. This leads to government's need to gain more control and visibility over systems.

FACING UNIQUE CHALLENGES

As discussed earlier in this chapter, managing the complexity of security in tandem with competing demands from regulators, citizens and other government departments are the overwhelming challenges facing public sector managers today, as they navigate toward a robust, yet flexible, IAM solution. This important role of protecting and serving is made more difficult by legacy systems, a fragmented approach to public sector management, and the lack of accepted industry standards.

Many of these challenges are unique to government, as illustrated in Figure 2:

FIGURE 2

Government Enterprises Fundamentally Differ from Businesses

Mission:

- National Security
- Citizen Service/Originator of ID
- Protection of the Citizen
- Enabler of Commerce
- Fundamentally different types of transactions, examples: Voting, Births, Deaths, Immigration, Defense, Criminal Prosecutions, etc.

Rules:

- Many laws apply differently to governments than to private enterprises (FISMA, etc.)
- Citizens fundamentally expect governments to protect them as well as expect to be protected from governments
- Rules are both legal (laws) as well as cultural, vary significantly from country to country

Scale & Complexity:

- Usually much larger than the enterprises within country
- Lack of centralized management of infrastructures
- Complex high-level security environments

The existence of legacy systems purchased and installed over many years provides a major hurdle for many governments. These systems will take years to transform, replace or upgrade. The inflexibility of these systems is being exposed, as governments face a whole new set of demands to share information between agencies and to more fully understand and utilize data.

Governments have an increasing number of users that require access to its applications and data. This includes organizational partners (within multi-department organizations), customers (the citizenry) as well as contractors and suppliers. The growing variety of these users is a major problem.

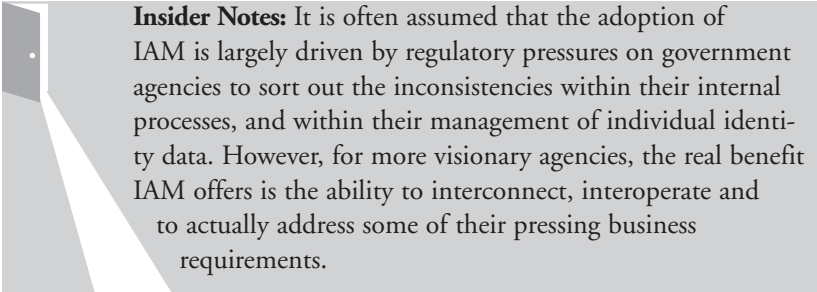
However, the biggest change in the last three to five years is that governments have had to open up their systems. Whether a government system is public and open, or high security, there has been an exponential growth in the number of users that need to access that information. It's analogous to

algae spreading on a pond. Combine this plethora of users with the growing number of applications that people need to access, both inter- and intra-departmental, and the management challenges become clear. Different classes of users with different security and control requirements exacerbate this complexity of volume.

In addition, governments are challenged by the desire to aggregate knowledge from a variety of sources. This problem entails how to get legitimate access to this information and stop illegitimate access to it. Opening up access to data repositories is one objective, but controlling this access is more important. This leads to government's need to gain more control and visibility over systems.

There also is the citizen's side of this issue. As governments automate customer-facing systems, such as the issuance of driver's licenses, and then correlate this information with passport and other data, they must convince citizens that this information is needed and will be used for the good of the citizenry. How can this be done without inflaming public interest groups that inveigh against Big Brother and Big Government? One way is to demonstrate, that although this personal information is being shared, there are visible and auditable controls that not only expedite the free flow of data, but also protect citizen privacy.

Another major challenge to general IAM implementation is the lack of comprehensive standards. There is now a real urgency to find a common solution. Notably, the U.S. Department for Homeland Security (DHS) wants, and needs, to work with different departments, but they don't nec-

A grey callout box with a white dot in the top left corner, containing the text of the 'Insider Notes' section.

Insider Notes: It is often assumed that the adoption of IAM is largely driven by regulatory pressures on government agencies to sort out the inconsistencies within their internal processes, and within their management of individual identity data. However, for more visionary agencies, the real benefit IAM offers is the ability to interconnect, interoperate and to actually address some of their pressing business requirements.



REAL SUCCESS

Farsighted governments worldwide are viewing IAM as a catalyst for effecting far-reaching and beneficial change in how they secure assets, serve citizens and protect national interests. Below is an example of how IAM has been successfully utilized by a major government in Europe:

■ The Belgian Federal Government

The delivery of services to citizens via efficient and accessible eGovernment systems is a clear imperative for high performing governments, especially in developed countries. In an effort to improve service delivery efficiency and effectiveness, without sacrificing security or public privacy, the federal government of Belgium is implementing broad-based eGovernment services supported by solid user authentication capabilities.

This multi-year project involves national, regional and local government structures. The implementation maintains the fine balance between convenient anytime, anywhere service delivery and the need to foster public confidence and a continued sense of privacy among citizens.

The Belgian federal portal hosts the state-of-the art identity management system, which is linked to personal electronic identity cards or token cards for citizens and civil servants. As the cornerstone of the eGovernment program, the security system enables the federal government to authenticate citizens and civil servants.

Accenture worked closely with the Belgian federal government to build the core eGovernment system, and led the design and implementation of a federated authentication service. It is designed to enable secure single sign-on to applications within and between organizations. The Belgian government implementation consists of a SAML provider supporting the browser/artifact profile hosted at the Belgian federal portal.

The federated authentication service improves security for eGovernment service providers by means of a nationally recognized user authentication standard. In addition, it makes a limited, customizable set of nationally relevant user attributes available to whichever department acts as the

service provider. Each service provider can implement customized access rules or personalize the service on the basis of these user attributes.

All levels of government and other third parties can use the federated authentication service, to enable eGovernment services that require strong user authentication. This brings inherent economies of scale, reduces unnecessary duplication and improves the efficiency of state expenditure.

For 2005, over half a million tax returns will be filed electronically by people using their electronic ID or token to prove that they are who they claim to be. The Ministry of Finance did not have to invest in an expensive identity management system to make this possible.

A significant benefit is the substantial cost reduction for service providers that require access to a user authentication capability to offer eGovernment services. The federated authentication service means they do not need their own user registration, management and authentication processes. This benefit includes peripheral cost savings, such as eliminating the need for their own helpdesk support for credential management.

Perhaps most significantly, the federated authentication service of the Belgian federal portal is a great vehicle for providing a seamless, user friendly experience for citizens and civil servants alike when they consume eGovernment services. They can peruse the same authentication credential across a wide range of security domains that have chosen to trust the federated authentication service of the Belgian federal portal. These benefits create a strong incentive for other layers of government and beyond to realize the vision of rich eGovernment services for citizens and civil servants.

essarily have the control or authority over how to do this. If there were standards in place, this would not be a problem.

Therefore, as is often the case, the technology, the thinking and the application of IAM is currently ahead of the standards bodies working to control it. The lack of a consistent security framework, especially in govern-

ment agencies, is another security challenge. To meet these challenges, an IAM system must be able to align those processes and technology solutions to allow the consolidation and integration of different types of identities within one management structure, and provide individualized security rights based on a person's identity

IAM AS A CATALYST FOR CHANGE

Most organizations appreciate the advantage of IAM. Nonetheless, some argue that its implementation engenders real and profound implications for the unique and difficult challenges that governments face. Although an organization might save \$10 to \$15 million a year with IAM, it may also incur additional risk while making these changes. IAM is a significant change agent in any organization and it touches almost everything within the enterprise.

Organizations tend to be nervous about large programs that bring change. However, smart government managers are embracing the positive change made possible by IAM, with tangible results. Below is a summary of these case studies.

■ The U.S. Department of Homeland Security

In June 2004, the department selected Accenture to lead an alliance to design and implement the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program, which will help manage the entries and exits of non-US citizens, verify visitor identities and support visa and immigration compliance.

US-VISIT will help secure America's borders while facilitating trade and travel, as well as ensure the integrity of the immigration process while protecting individuals' privacy — all defined by jointly determined measures. Together, U.S. Department of Homeland Security officials and the Accenture-led team, called the "Smart Border Alliance," are working with stakeholder agencies to design a system that transforms border management through the integration of databases, streamlined procedures, international data-sharing efforts and biometric technologies that support the work of U.S. officials at home and abroad. A signature feature is the planned devel-

opment of a new type of person-centric, electronic profile that provides real-time information on the status of visitors to the United States.

■ **Belgium.** The federal government of Belgium is implementing broad-based eGovernment services, supported by solid user authentication capabilities, in an effort to improve service delivery efficiency and effectiveness without sacrificing security or public privacy. This multi-year project involves national, regional and local government structures. The implementation maintains the fine balance between convenient anytime/anywhere service delivery and the need to foster public confidence and a continued sense of privacy among citizens.

■ **Ireland.** The Office of the Revenue Commissioners (Revenue) has developed its systems to provide an easily accessible and unified view of their customers. This integrated approach has provided the platform for innovative online tax services, mainly aimed at businesses and the self employed, that allow payment and filing of taxes via the Internet using PKI based security. This has recently been complemented by non-PKI channels, such as SMS, IVR and web forms, for low-risk personal transactions. In the next iteration, Revenue will combine identity and registration security from the Reach agency (which provides the national public service broker) with its own PIN security to offer services to the 2m PAYE employees. Revenue Ireland is one of the few agencies worldwide to combine online service with an integrated back-end solution, thus ensuring its customers a seamless overall service.

■ **Spain.** The Spanish Ministry of Labor and Social Security is making radical changes to its welfare and health services by issuing a new social security smart card for all dependents. The project was rolled out in Andalusia,

Insider Notes: The lack of a consistent security framework, especially in government agencies, is a real security challenge. To meet these challenges, an IAM system must be able to align those processes and technology solutions to allow the consolidation and integration of different types of identities within one management structure, and provide individualized security rights based on a person's identity.

a large region in southern Spain, and is accessible to 7 million users. Citizens are able to use the card at self-service terminals, or kiosks, around the country, to take care of routine administrative tasks as well as more personal business. As a security measure, the terminals use fingerprint identification technology, allowing citizens to access sensitive information.

LOOKING TO THE FUTURE

The general trend in IAM is towards consolidated identity. Many countries have announced plans for eServices cards or national IDs, or for multipurpose cards by which citizens hold digital certificates. The main reasons given to citizens for the issuance of these identifications are the fight against terrorism, reduction of identity theft and better access to eGovernment services.

There exists a clear need for stronger, automated, interoperable and online identity. Using traditional documents, designed for other purposes, opens too many doors to security flaws. For example, a U.S. Social Security number is an identifier, not a proof of identity (i.e., not a shared secret); a birth certificate is generally used for statistical purposes, not as proof of identity; driver's licenses assert the passing of certain physical, mental and skill tests which suggest the ability to safely operate a vehicle of a given class. None of these were designed to assure identity.

We need:

- Stronger identity to cope with globalization and combat organized crime
- Automated and interoperable identity to cope with globalization and deliver high-performance
- Online identity to support eGovernment and eCommerce

The solution:

- Multiple factors, biometrics
- Electronic format for automated and network-based validation (web, phone, email)
- Should still enable face to face, human validation, as fallback/transition procedure
- Increased emphasis on enrollment

While biometrics is not the silver bullet for identity management, it is currently the only way to heighten security and improve efficiency in eGovernment, especially in border control/immigration. The optimal practice for security entails three interrelated factors:

- 1 something you have (a card)
 - 2 something you know (PIN/password)
 - 3 something you are (biometrics)
-

There is general movement towards electronic ID with multiple biometrics and PKI to automatically identify, authenticate and fill the online identity void for government employees, citizens and the private sector.

Here are examples of notable large-scale pilots and implementations of online identity already underway:

- National ID: U.K., China
- Public service card: Ireland, Denmark
- Multipurpose ID card: Japan, India, South Africa, Belgium, Italy

Culture and historical issues as well as data protection and privacy laws could lead to different implementations of this solution, such as:

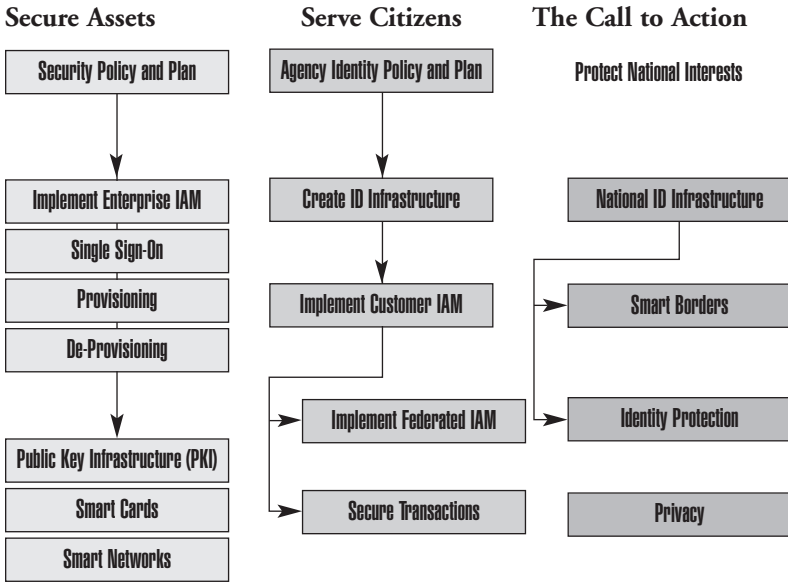
- Centralized vs. federated identity infrastructure
- National ID vs. public service card vs. multipurpose ID card
- Compulsory vs. voluntary implementation

SETTING OUT A ROADMAP FOR IAM

Reaching an IAM solution will require various steps. Governments must first conduct a comprehensive analysis of their identity management processes and security needs. To make sure their development is comprehensive and shared, solutions should be assessed relative to the security practices of partner agencies, governments and organizations.

IAM solutions share a common set of capabilities. However, IAM's implementation differs greatly among Internal IAM (Secure Assets), External IAM (Serve Citizens) and National IAM (Protect National Interests). Figure 3 illustrates specific roadmaps for governments to follow in establishing an IAM solution to address these three priorities.

FIGURE 3 IMPLEMENTATION ROADMAPS:



Governments must help educate the public regarding the benefits of effective identity management, assuaging whatever anxieties exist regarding privacy. The public and private sectors also must cooperate and take advantage of their complementary IT capabilities as much as possible, to identify common IAM methods.

This public-private approach will generate synergies by which the sum of the parts is greater than the whole, spawning truly remarkable solutions. An environment of partnership will give birth to many of the tools, processes and (just as importantly) the attitudes that are necessary for successful identity and access management. Make no mistake: to overcome the inevitable institutional biases against new ways of thinking, attitudinal change is vital.

To unlock identity's best and highest uses, IAM must transcend security. Identity not only keeps cyberwolves from the door, it also can deliver innovative, high-performance solutions that efficiently speed the delivery of products and services to trusted individuals.

In this new era of identity management, citizens will see security features not as a burden or a source of fear, but as a means of protecting and leveraging their most important asset — their identity.



Dr. Alastair MacWillson is the Partner in charge of Accenture's global Security Services and works with business and government leaders on security, trust, privacy and compliance. He also serves on the leadership team of Accenture's global Technology & Outsourcing Service Line. Prior to joining Accenture, Alastair spent 16 years with the U.K. Foreign Service, conducting international risk analysis. Alastair holds a doctorate in Theoretical Physics, related to research in Applied Cryptography. He can be reached at: alastair.macwillson@accenture.com

Eric Stange has 25 years experience in information technology and management consulting. For the past 14 years he has focused on serving the U.S. Department of Defense in a variety of business areas, with a specific emphasis in the logistics and supply chain area. More recently, Eric has taken on leadership of Accenture's Defense and Homeland Security portfolio, which includes the DoD and Department of Homeland Security. Eric holds a B.S. degree in Commerce. He can be reached at: eric.s.stange@accenture.com.

Company Name:	Accenture
Address:	11951 Freedom Drive
City:	Reston
State:	Virginia
Zip:	20190
Phone:	312-737-8842
web site:	www.accenture.com

DESCRIPTION

Accenture is a global management consulting, technology services and outsourcing company. Committed to delivering innovation, Accenture collaborates with its clients to help them become high-performance businesses and governments. With deep industry and business process expertise, broad global resources and a proven track record, Accenture can mobilize the right people, skills and technologies to help clients improve their performance. With more than 126,000 people in 48 countries, the company generated net revenues of US\$15.55 billion for the fiscal year ended Aug. 31, 2005.

SERVICES

Accenture has more than 1,100 security professionals helping organizations work through complex security issues such as strategy, compliance, identity and business continuity. Accenture helps organizations deliver increased performance and sustainable cost reductions across the security spectrum. Our Security offerings describe the breadth of solutions that we currently bring to clients.

Securing the Extended Enterprise

- Identity and Access Management
- Secure Web Services
- Secure Data and Rights Management
- Secure Business Application Platforms
- Next Generation Secure Networks
- Secure Mobility

Preventing High-Cost Security Failures

- Security Risk Management and Assessment
- Embedded Business Continuity

Driving Operational Excellence

- Security Strategy and Transformation
- Security Governance and Organization Design
- Effective Privacy and Compliance

Transforming the Security Function

- Security Management Services
-