IBM Global Business Services

IBM Institute for Business Value

Government

Identity management in the 21st century

Balancing safety, security and liberty in a global environment

IBM Institute for Business Value

IBM Global Business Services, through the IBM Institute for Business Value, develops fact-based strategic insights for senior executives around critical public and private sector issues. This executive brief is based on an in-depth study by the Institute's research team. It is part of an ongoing commitment by IBM Global Business Services to provide analysis and viewpoints that help companies realize business value. You may contact the authors or send an e-mail to iibv@us.ibm.com for more information.

GBE03250-USEN-00

Identity management in the 21st century

Balancing safety, security and liberty in a global environment

By Bryan Barton, Dennis Carlton and Dr. Oliver Ziehm

Effective identity management is becoming a critical issue with governments worldwide as more and more people travel and seek access to services on a daily basis. Questions surrounding the integrity of identity documentation, as well as the lack of consistent and effective means for nations to exchange identity information, often leave gaps that can be exploited by criminals, organized crime syndicates and terrorists. Governments should move immediately to develop and implement improved identity management solutions that enable quick and accurate identity information exchange, while protecting individual privacy rights and civil liberties.

Balancing the growth in global travel against the escalating threat of identity fraud, illegal immigration, international crime and global terrorism has driven many nations to invest in measures to improve identity management. The increasing demands of globalization – in which products and services, and the people who provide them, must move expeditiously across international borders – have prompted a closer examination of the effectiveness of some of these programs. Many governments have invested in "smarter" drivers' licenses, passports, automated border control systems and visas, resulting in more secure forms of identification, but have often done so without much consideration for their impact on a nation's overall identity strategy.

Additionally, identity management programs ideally include safeguards for public health and safety – as well as creating mechanisms for enhanced government services and the

preservation of individual liberties, such as privacy and individual data security. But in reality, many governments are finding their programs ill-equipped to provide the various protections and services for which they were supposedly designed.

Despite significant strides in improving and standardizing identification documentation, governments today still have difficulty ascertaining the true identities and legitimacy of those who hold these documents. Political concerns, organizational inefficiency, privacy and legal issues, and legacy technology systems all impede the effectiveness and efficiency of identity management programs. As well, many of these programs lack a cohesive structure and face challenges in collaboration and communications – both internally and internationally.

In the absence of a comprehensive national strategy, governments also cannot be certain the identity data entrusted to their care is either secure or private. Based on recent research conducted by IBM, we believe it is time for both governments and the private sector throughout the world to take a new look at identity management and explore ways to facilitate communication and collaboration among government, industry and society. Our findings tell us that maintenance of the *status quo* – taking no action to address the shortcomings and gaps in various disharmonized national identity management programs – creates increased risk and exposure to international crime, identity fraud and illegal immigration.

As part of our research to identify the challenges and opportunities in creating more comprehensive national identity management programs, the IBM Institute for Business Value conducted a study of identity management policies of various governments around the world. Employing a carefully structured survey document, IBM executives interviewed a wide range of government thought leaders in the Americas, Europe and Asia to ascertain their views on identity management leading practices. In addition, IBM subject matter experts augmented the primary research by consulting scholarly papers on identity management topics published by government, academic and industry experts.

The establishment of a cohesive national identity strategy requires clearly delineated goals and expectations supported by the right mix of people, processes and technology, both in the public and private sectors. Whether or not such a strategy currently exists – or is in the process of being formulated – we believe governments should take immediate action to improve data integrity, system security and constituent privacy.

Identity management in the 21st century

Balancing safety, security and liberty in a global environment

Impediments to progress

Piecemeal pervades

A cohesive national identity management strategy is not common among the large, market-driven democracies that represent the bulk of the countries that participated in our survey. Not surprisingly, many of those countries that feel the greatest sense of urgency to strengthen national identity management programs are those that have suffered recent acts of terrorism.

While many nations are working to establish identity management programs, issues with collaboration and accountability often slow progress.

With only a few exceptions, most leaders in our survey countries have seen their identity management strategies evolve out of a variety of legislative initiatives and regulatory decisions implemented by multiple and disparate government agencies. Working without an overall plan, these nations have devised piecemeal, often narrowly focused identity management approaches in response to specific national security, immigration control, privacy protection and other societal concerns. Among the countries we researched, we found that current approaches to identity management span the spectrum from no national plan in place to those that are holistic but only partially implemented.

Many nations, in fact, are now in the process of implementing various initiatives, but have realized little harmonization. A number of issues combine to delay identity management improvement. The political model in place in the individual country, as well as its various international and multinational agreements, often slows progress. For example, in some instances sovereignty over identity-related data is vested in individual states within a country, thereby complicating or preventing national-level identity management collaboration. As well, accountability becomes an issue – as task responsibilities related to identity management are often split among various governmental departments, making it difficult to identify the accountable entity with overview responsibilities.

Of the many nations we surveyed, two countries, the United Kingdom and the United States, illustrate the range of approaches toward identity management policy. For several years, the United Kingdom has been in the process of developing and refining a top-down national identity management strategy and has created a National Identity and Passport Service that serves as the sole entity responsible for identity management strategy, policy and core areas for delivery.[1] The United Kingdom is moving toward establishing a national identity card, which will serve as the foundation for all identity policies within the country. To offset the considerable expense generated by a cohesive national identity management program, U.K. leaders are considering collecting fees from the private sector when it uses the card for identity confirmation.

By contrast, the United States has adopted national-level legislation that mandates improved identity management policies and procedures, but leaves many implementation decisions to the various federal agencies (for example, Homeland Security Presidential Directive 12) and state governments (e.g.,

the Real ID Act). The hub of this strategy is information sharing – making sure information about known threats is shared as early as possible within the U.S. Department of Homeland Security (DHS) and with agencies of other governments. Most of the cost of the American program will be borne by the individuals who obtain the identity documents.[2]

Whether centrally managed or widely distributed, identity schemes frequently generate political and public controversy. But citizens still expect their governments to protect them from crime, terrorism and identity theft.

Austria's central register provides wide view of relevant data[3]

Austria has created a central register of residents to assist in its identity management endeavors. The *Zentrales Melderegister* (ZMR) is a central database with a wide view of relevant resident data. Its goal is to simplify identity administration and enable a one-stop government. This database is the basis for voter registration, population census, citizen card, financial equalization, infrastructure planning (streets, schools) and more.

Every Austrian has the obligation to register with the local authorities within three days of moving to a new address and to cancel the old address record. Austria's 2,357 cities and communities update the information in this register online in realtime. Every Austrian public authority has 24-hour online access to the following data: name, gender, birth date and place, registry number and nationality.

Generally, every person with justifiable reason has the right to receive public information about registered citizens, but has to pay a certain fee.

Additionally, certain certified business partners (banks, insurance companies, lawyers, debt collection agencies) have the opportunity to make automated online requests for information.

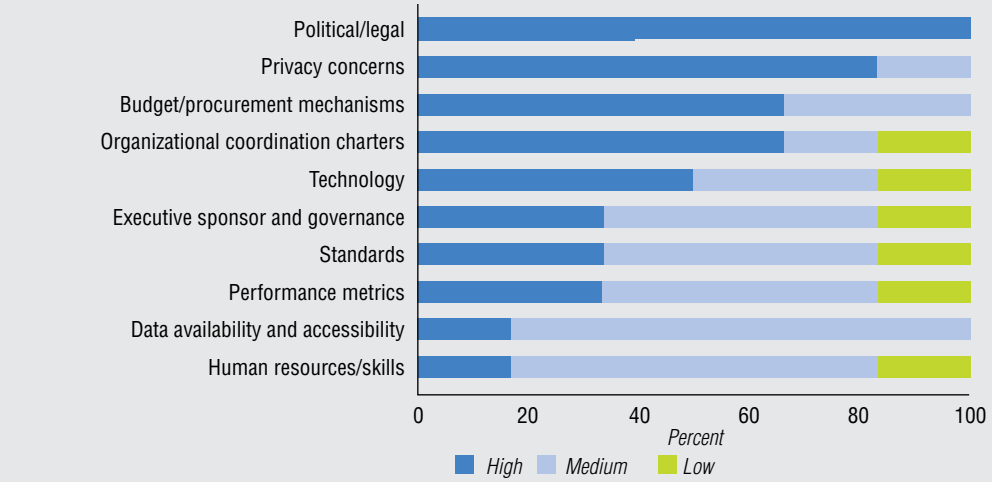
Barriers – Political, privacy and budgetary issues slow progress

Despite the widely recognized need for improved national identification solutions, several key barriers continue to prevent them from being fully realized. Our survey identified some common concerns among government identity management thought leaders (see Figure 1). Chief among these is the potential political fallout associated with addressing such a controversial issue. Identity management and its resulting impact on personal liberty and privacy is an extremely sensitive subject, particularly in the world's developed democracies. Officials concerned about reelection often avoid identity management issues altogether, as they often lend themselves to potential negative media coverage and public attention.

Survey respondents also cited the privacy policies and regulations of individual governments as a significant barrier to information exchange and identity management, especially when countries must share a traveler's personal data as part of an international border management transaction. While some decry identity management programs as examples of a decline in a government's respect for individual privacy, we believe it is the lack of consistent policies and methods of information exchange that encourages identity theft, which is among the most significant threats to personal privacy.

Another barrier noted by respondents is the limits inherent in legacy IT systems that lack the ability to effectively administer complex and coordinated national programs. This problem is magnified by the fact that overall budgetary and procurement constraints also contribute significantly to the piecemeal

FIGURE 1.
Roadblocks to identity management programs – Respondents rate the severity of various barriers to improved identity management strategy.



Source: IBM Institute for Business Value Identity Management Survey.

systems currently in place in most countries. Additional obstacles include the varying standards from program to program and nation to nation, lack of consistent, measurable performance metrics, lack of access to necessary data and a lack of skilled people to design/implement such a system.

Legal, regulatory and cultural barriers often preclude the collaboration necessary between the public and private sectors to create comprehensive identity management strategies.

Collaboration – or the lack thereof

In many countries, legal, regulatory and cultural barriers significantly limit or preclude government and the private sector from collaborating to achieve more comprehensive identity management strategies. Because of information and security issues, it's difficult or illegal in many countries for governments to contract administration of identity management programs to commercial entities. One survey respondent said his country actually considered the lack of a cohesive national identity policy, along with the persistence of identity silos, as enhancing the protection of citizens' sensitive identity data. For the most part, collaboration on identity management issues is limited to technical research, expert groups and standards definition efforts.

Information (in)security

No matter how sophisticated the technology, most countries have concluded that IT alone cannot provide sufficient privacy-protective solutions to satisfy the expectations of governments and societies. Despite the advent of readily available security solutions such as smart card-based strong authentication, employee-facing biometrics and rule/role-based data security, the leaders we interviewed in various countries felt these measures were not sufficient to provide high-integrity identity data management. Regardless of the level of sophistication of the IT infrastructure, most countries prefer to apply extensive employee training combined

with layered security processes as their primary means for protecting the integrity of identity management. The challenge ahead for governments will be to make effective use of today's security technology when integrating legacy applications to create an open, flexible architecture that helps maintain data security and increases interoperability.

Steps toward improved identity management

Because the threats from international crime, illegal immigration, terrorism and identity theft are not expected to diminish over time, governments must take steps to create or evolve an identity management process – even if there is no "stated" national strategy. Maintaining the *status quo* is not an option.

Many identity management schemes are initially justified for their perceived ability to reduce crime and prevent terrorism. However, the experience of governments has shown that such mandates are a relatively weak justification in their own right for making a long-term investment in identity management solutions.

Political leaders can overcome or mitigate the fallout from implementing these programs by demonstrating the numerous ancillary benefits provided to the domestic populace – such as those gains realized by Danish citizens in their country's e-government facilitation model (see sidebar, Radically different objectives drive identity management programs). Enhanced benefits from a cohesive national program could include more timely delivery of government benefits, elimination of redundant identity information and increased benefits resulting from the prevention of fraudulent claims. Investments in identity management solutions are much easier to defend when the media and public grasp their beneficial nature. Strong leadership with a long-term focus is needed to push both domestic and international collaboration and create a perception of balance and fairness.

Based on the current state of identity management programs throughout the world and the perceived need for more aggressive action by leaders in many nations, we have developed the following specific recommendations

Radically different objectives drive identity management programs

Most identity management systems in place today lack a comprehensive focus and are designed to achieve a narrowly defined set of objectives. Two prevailing models are in place today.

The model used in the United States is based on security enhancement and focuses on reinforcing immigration control and increasing national security. DHS was created for this purpose and has as a primary objective the elimination of terrorism. DHS serves as a focal point through which information is gathered and distributed.

Other nations, however, use identity management programs to facilitate e-government. Denmark, for example, uses this model to enable ease of access and help deliver social services to its population.[4] The Danish Civil Registration System (CRS), which provides Danes with a personal identification number that can be used when interacting with the government, is an example of how a consolidated IT infrastructure can manage public information. The entire Danish public sector uses the identification numbers provided by CRS for administrative purposes. In addition, CRS data can also be used by the private sector for a variety of purposes under arrangements tightly regulated by the Danish government.

Improved security and enhanced privacy are not mutually exclusive – a fact governments should communicate to their respective populations.

to help facilitate the establishment of cohesive and collaborative identity management programs:

1. Government agencies and organizations should work in parallel to adapt and/or update legislation and regulations and work to establish cohesive identity management processes. Regardless of whether a government has implemented a comprehensive identity management strategy, we believe all governments should adopt immediate legislative and regulatory measures to enhance the integrity, security and privacy of their identity management schemes. Measures that have been implemented successfully by some countries include the creation of technical working groups to explore avenues for more secure, privacy-protective data exchange combined with the creation of oversight committees to represent/protect the interests of government, the private sector and society. Synergies can be realized by carefully consolidating initiatives on various governmental levels via oversight task forces comprised of key technical, security, privacy and governance stakeholders.
2. Governments should implement flexible systems and technology that can tolerate uncertainty and provide for future changes driven by new technology or international agreements. Modern IT solutions that embrace compliance with governmental and commercial standards make intergovernmental collaboration easier. Implementing standards-compliant solutions helps make systems more future resistant. Service-oriented architecture solutions (SOA) allow governments cost-effective ways to extend the service life of existing applications and databases – while simultaneously injecting new functionality, capacity, precision, throughput and flexibility. Powerful new text searching tools can help resolve identity issues by recognizing alternative spellings of names, as well as uncovering non-obvious relationships among people who appear otherwise unconnected. These new techniques and tools allow governments to better leverage legacy solutions, while establishing a foundation for privacy-sensitive identity management that is more accurate and more secure.
3. Governments should also realize – and communicate to their respective constituents – that improved security and enhanced privacy are not mutually exclusive goals. Privacy expectations differ from culture to culture – as do expected government roles in protecting individual privacy. Systems must be designed to accommodate these differences. All changes in identity management policies should include a sustained commitment to leading governmental and commercial technology, privacy and security practices. Privacy protections should be embedded within the core architecture of an identity management system, not appended as an afterthought. In a market-driven democracy, citizens expect government to sustain the integrity and privacy of the identity data in all domestic and international transactions. Any significant breach of trust is likely to have consequences for a freely elected government. However, governments must realize any system, no matter how comprehensive and well-designed, will

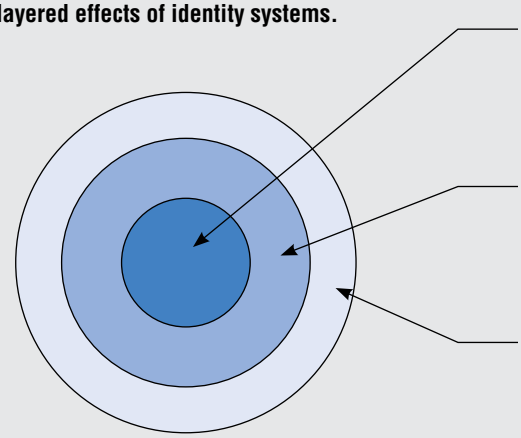
occasionally generate errors. Citizens whose identity data is misused – for example, being mistakenly denied access to commercial aircraft – will find it difficult to restore their reputations without government intervention. Therefore, identity management systems should include simple and fast remedial mechanisms and measures to correct errors and maintain public confidence.

4. As with any endeavor of this magnitude, governments should have a clear definition for the goals of all identity management measures undertaken. The design of a comprehensive identity management program must be in line with its results. We believe governments should resist the type of "mission creep" that results from solutions or methodologies that first attempt to identify everyone within its borders and then try to find ways to make use of that data. Such an approach often undermines public support for identity management programs and instills a sense of unease and uncertainty in the populace. As a result, we believe a transparent communications program is essential to create and maintain a high level of trust among constituents. The benefits of effective identity management – improved service delivery, simplified identity authentication, reduced identity theft – should be clearly articulated to a government's constituents.

The positive benefits of identity management extend well beyond basic border management

Identity management solutions generate positive ripple effects for service delivery throughout many levels of the government and the private sector. As shown in Figure 2, there are several "identity-dependent" initiatives, such as transportation safety, immigration control and regulatory compliance, that form the basic foundation of identity management services most governments provide their constituents. Often not as well understood are the many other public and private services these foundational identity services support. Immediately outside these identity-dependent functions is a range of "identity-enhanced" initiatives that benefit from investment in improvements in core identity systems and methods. Beyond these functions are many "identity-supported" initiatives, primarily in the private sector, such as financial transactions, e-commerce, digital signatures and watermarks, that benefit when a government improves core identity management functions.

FIGURE 2.
The layered effects of identity systems.



Identity-dependent initiatives
- Transportation safety
- Border crossing, immigration control
- Regulatory compliance

Identity-enhanced initiatives
- Facilities and data access
- Transaction auditing and monitoring
- Identity theft and fraud prevention

Identity-supported initiatives
- Financial transactions, eCommerce
- Digital signatures, watermarks
- System security and privacy

Source: IBM Institute for Business Value.

Lack of a collaborative approach will likely leave governments vulnerable to numerous security and privacy breaches.

Australia addresses identity management shortcomings

In 2005 Australia was rocked by two high-visibility cases that underscored how previous processes and systems were unprepared to resolve difficult identification challenges. One was the case of a naturalized Australian citizen who was unable to communicate her identity or status to law enforcement and immigration officials and ended up being deported to her native Philippines.[5] The other case involved a naturalized Australian who was an undiagnosed schizophrenic that authorities held in custody for ten months as they struggled to identify her and understand her mental state.[6] Independent commissions formed to investigate these cases found flawed processes, ill-trained staff and "siloed" identification systems unable to communicate with one another.

The Australian government took swift, decisive action to respond to the recommendations of these commissions. Recognizing the importance of implementing a "holistic corporate case management system," the Australian Department of Immigration and Multicultural Affairs, now known as the Department of Immigration and Citizenship (DIaC) launched its "Systems for People" program to transform the way the department does business.[7] The Systems for People program provides a set of easy-to-use portals to improve access to services and allows DIaC staff a more complete view of a client's case by tapping into many identity-related applications and databases from a single screen. In combination with improved administrative and detention policies and better-trained staff, the Systems for People program helps DIaC deliver on its mission to "enrich Australia through the well-managed entry and settlement of people."

Questions to ponder

Governments that fail to consider more collaborative approaches toward identity management issues are likely to remain vulnerable to security and privacy breaches from innumerable angles of attack. All levels of government must work in unison to inform the populace about the risks of leaving identity management as an *ad hoc*, unplanned occurrence. As a starting point, research suggests government agencies might consider the following questions:

Improved governance – What measures can we take to make enhancing identity management across all levels of government a higher priority? What is our cross-government identity management strategy? What laws or regulations must be modified to spur greater inter- and intra-governmental collaboration?

New standards and technologies – With which standards-setting bodies should our government engage to help define and implement identity management standards compatible with our goals and culture? Are we exploring new technologies to improve search accuracy, data integrity, data security and constituent privacy?

Security, privacy and data integrity – What steps can we take to better accommodate the goals of both security experts and privacy advocates? What can we do to help citizens and travelers have easy access to multiple channels for correcting identity-related errors in realtime?

Clear goals – How can we more actively engage society, including the media, in the identity management decision-making process? What tangible benefits (e.g., enhanced and expedited service delivery, reduced fraud or revenue generated by transactions made more secure by identity management) can be linked to investments in improved identity management strategies?

The answers to these questions can help identify immediate measures that can result in improved identity management processes. These processes can assist governments in their continuing efforts to protect their citizens, deliver better service and preserve the integrity, security and privacy of sensitive identity data.

About the authors

Bryan Barton is Vice President and Partner for IBM Global Business Services and a leading expert on border management. Bryan is responsible for IBM solution development in the areas of customs, ports and border management and works closely with governments around the world. He has coauthored numerous articles including: "Balancing and optimizing trade facilitation and border integrity – Strategies and options for the global customs agency community" and "Expanded Borders and Integrated Controls – Achieving national prosperity and protection through integrated border management." Bryan can be contacted at *bbarton1@us.ibm.com*.

Dennis Carlton is a Strategy Consultant on the identification industry for IBM Global Business Services. Denny has more than 20 years of experience leading the development of complex IT systems and products, including the development of automated fingerprint identification systems and single- and ten-finger identity scanning and matching solutions. Additionally, Denny led an extensive study of biometrics and border management. Denny can be reached at *dennis.carlton@us.ibm.com*.

Dr. Oliver Ziehm is a Managing Consultant with IBM Global Business Services. With 15 years experience in public sector consulting, Oliver now works for the IBM Institute for Business Value. In this role, he is responsible for the creation of global studies on strategically relevant issues for the public sector. Previously, he worked with different authorities at the federal, state and community level (e.g., police, school administration and universities) as well as the healthcare sector. Oliver can be reached at *oliver.ziehm@de.ibm.com*.

Contributors

Norbert Kouwenhoven, SBS Solutions Leader Customs, Ports & Border Management, IBM Global Business Services.

Paul McKeown, Business Development Executive, Customs, Ports and Border Management, IBM Global Business Services.

Andreas Pohler, Partner, Customs, Ports & Border Management, IBM Global Business Services.

Poh-Ling Lee, Associate Partner ,Custom Development, IBM Global Business Services.

Carlos Santos, Associate Partner Public Sector, Business Development Executive, IBM Global Business Services.

About IBM Global Business Services

With business experts in more than 160 countries, IBM Global Business Services provides clients with deep business process and industry expertise across 17 industries, using innovation to identify, create and deliver value faster. We draw on the full breadth of IBM capabilities, standing behind our advice to help clients implement solutions designed to deliver business outcomes with far-reaching impact and sustainable results.

References

1 "About ID cards and the National Identity Scheme." United Kingdom Home Office. Identity & Passport Service. http://www.identitycards.gov.uk/scheme-what.asp

2 "The Real ID Act: National Impact Analysis." National Governors Association. National Conference of State Legislatures. American Association of Motor Vehicle Administrators. September 2006. http://www.ncsl.org/print/statefed/Real_ID_Impact_Report_FINAL_Sept19.pdf

3 ZMR Info, Zentrales Melderegister, Austrian Home Office. 2005. http://zmr.bmi.gv.at

4 "The Civil Registration System in Denmark." Det Centrale Personregister. September 27, 2001. http://www.cpr.dk/cpr/site.aspx?p=198&areaid=27&ArticleTypeID=76&t=visartikel&Articleid=4327

5 "Australia reviews detention cases." *BBC News*. May 25, 2005

6 Ibid.

7 "Systems for People." Australian Department of Immigration and Citizenship. http://www.immi.gov.au/about/department/perf-progress/dima-improvements/faq/bcs-it-reform/faq2.htm

© Copyright IBM Corporation 2007

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
10-07
All Rights Reserved

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

G510-7859-00