

Use Cases for Identity Management in E-Government

E-government identity management systems aren't usually straightforward to implement. Culture and history strongly affect what might be acceptable to citizens in particular circumstances, with levels of trust being a key factor. The authors discuss these issues and present a use case from New Zealand.



Across the globe, governments are strengthening their identity management strategies. One reason is a growing interest in using the online environment to deliver and improve services, and another is the increasing sophistication of criminal elements in forging and stealing identities. Governments are also concerned about terrorism, including the use of money laundering to finance it.

This article focuses on the specific issues that arise when governments turn to e-government and use identity management to provide online services. Governments approach identity management in considerably different ways, so it's useful to assess these differences against historical and cultural backgrounds. Social policy can be as important as technology in determining an approach to identity management.

Ultimately, we're practitioners, not researchers, so this article isn't a systematic cross-governmental study. Rather, it draws on our in-the-field experiences from advising on and implementing e-government identity management systems in Australia and New Zealand. When we speak of identity management here, we use the definition adopted by the Australian government: "the policies, rules, processes and systems involved in ensuring that only known, authorised identities gain access to networks and systems and the information contained therein" (www.agimo.gov.au/infrastructure/authentication/agaf/glossary/i#identitymanagement).

Is government different?

Those who develop use cases for identity management might assume that there isn't much difference

between the issues to take into account when building government versus private-sector use cases. This assumption has some validity, especially because of the increased partnerships and cooperation between governments and the private sector for service delivery. However, some key distinctions have an impact on the approach taken to develop a new identity management system.

The first is that government must look into much broader issues, including social inclusion, consistency, and interoperability. A private enterprise might target a particular demographic, but government programs must serve an entire population that spans an enormous range in terms of age, technical competence, language, and physical and mental abilities.

Governments also carry a big stick: even those with a democratic structure have the power of civilized or legal coercion, which means that citizens have few options if they don't like the way they receive an essential service or how they're required to interact with government. Their main way to respond is through general elections held every three to five years, but this is a very limited form of "marketplace" test. These factors might make it more difficult for the community to accept government-initiated identity management systems than private-sector offerings. To compensate for this lack of control, citizens might expect stringent accountabilities or greater transparency about security and privacy.

While convenient, efficient and accountable online service delivery is a key reason for having strong identity management—other reasons include law enforcement and national security, the use cases for

ROBIN
MCKENZIE
AND MALCOLM
CROMPTON
*Information
Integrity
Solutions,
Australia*

COLIN WALLIS
*State Services
Commission,
New Zealand*

which differ from online service delivery. For law enforcement and national security, use cases might be about more easily and accurately tracking an individual or linking information about them to help with investigations. The disparity in these goals represents a reoccurring policy dilemma that governments face when they attempt to apply one identity management arrangement to more than one use case. Rather than try to meet all policy objectives with one solution, governments might need several identity management solutions.

Is e-government different?

The online environment allows for the collection and interconnection of larger amounts of information than ever before. This might benefit government—and possibly even citizens themselves—but it also creates several risks that didn't exist in more traditional paper-based systems. For example, government can much more closely track and monitor citizens' behaviors and use this information for a wide range of unexpected activities that might ultimately result in discrimination or inaccurate presumptions that could be both damaging and difficult to correct. In a commercial marketplace, citizens have the option to walk away from a service if they think the risk of using it is too high, but as we've mentioned, this isn't always an option in a government context. When citizens don't have a choice about the mechanism used to protect their privacy, governments have a particular responsibility for getting privacy and security right.

E-government also has the potential to blur accountabilities and responsibilities, which could make it difficult for citizens to receive redress. This blurring can be horizontal or vertical—for example, if a government online portal provides single sign-on services for several agencies, it isn't immediately clear which agency is responsible if the system fails. Similarly, responsibility for how well a system runs can fall under several parts of a government hierarchy, starting with the minister responsible for a particular agency down to the architect who designed it and the bureaucrats who approved and administer it.

In the absence of direct marketplace pressures, there is less incentive for government to be responsive to citizen concerns. However, when governments do implement measures to address online concerns, they often take great care to manage their own risks first. In the case of identity management, a glaring example often appears in government measures that avoid providing information, benefits, or services to the wrong person, but don't take equal measures to ensure confidence that citizens are interacting with legitimate government entities. Today, more governments are moving from using the Web to provide static information, such as how to vote or office locations

and hours, to much more significant services, such as renewing a driver's license, filing a tax return, or even voting. As the need for stronger online identity management has thus increased, the risks for the citizen of interacting with the wrong person have also risen and must be managed.

Governments are also exploring the use of interactive platforms and data analytics from the emerging Web 2.0 environment to seamlessly customize services and information for citizens and let them tailor the way they interact with their government. This technology might also let citizens participate more fully in policy development and service evaluation. Naturally, issues of identity and how to manage it become much more acute in this type of user-centric environment. Complicating the situation somewhat, government is currently the arbiter of the essential and authoritative processes for documenting identity in the first place, such as issuing birth certificates, passports, and other documents.

Approaches to identity management

How to manage identity online is a major preoccupation for governments and the private sector alike. Both have sought leverage—and have something to learn—from the other. Earlier efforts have either attracted major controversy or been forced back to the drawing board. Microsoft's Passport product, for example, received criticism because it gave the company too much control over users' personal information, and the UK's entitlement card initiative quickly turned into an identity card that ultimately lost public support once citizens learned the extent to which the government controlled it.^{1,2} A notable outcome of these types of efforts is the increased debate about the overall approach to identity management systems, which is moving beyond privacy as an abstract concept to a more concrete analysis of what actually concerns those who object to identity management measures.

Accordingly, the public and private sector are now producing a wider range of referential frameworks aimed at achieving consistency in designing privacy and security into identity management systems and, as a result, they are gaining greater community acceptance. The Australian government, for example, recently developed the Australian Government Authentication Framework for Individuals, or AGAF(I) (www.agimo.gov.au/infrastructure/authentication/agaf_i), and New Zealand debuted its "all-of-government" Authentication Programme (www.e.govt.nz/services/authentication). In a wider international context, the UK's London School of Economics has developed a set of best practice criteria (<http://is2.lse.ac.uk/idcard/>), Europe's Prime project is working on a published set of identity management principles (https://www.prime-project.eu/prime_products/whitepaper/), Microsoft's

Table 1. Separation of identity components in the New Zealand government’s identity information management system.

	KEY	KEY IDENTIFIER	FEDERATED LOGON TAG	IDENTITY
Key provider	X	X		
Government Logon Service		X	X	
Service agency			X	X
Service user	X			X

Kim Cameron has developed the “Laws of Identity” (<http://msdn2.microsoft.com/en-us/library/ms996456.aspx>), and the Eclipse open source community has developed the Higgins Project (www.eclipse.org/higgins).

Note that none of these approaches focus on compliance with privacy or data protection law. Supported by recent research that finds that the understanding and management of risks associated with online tools can be a determining factor in citizen acceptance of stronger identity management, we can best describe these recent initiatives as user-centric (<http://trustguide.org.uk/>). They focus on how to address the real concerns individuals have about what happens to their personal information in an identity management system and regard user control as central to achieving a solution that gains full user trust, usage, and acceptance.

A real use case: New Zealand

New Zealand has a population of 4 million people, served through 35 central public service departments and another 70 local and state agencies. The country has minimal national security or illegal immigration issues to combat, which narrows down the purposes and simplifies the considerations involved in providing online identity management systems. New Zealand’s e-government strategy has a goal for transforming online delivery of government services to the public by 2010 based on initiatives that support collaboration, standards, and interoperability.

The country’s Authentication Programme began in 2000, with an initial development effort that identified some key policy and implementation principles to guide the authentication solution’s design. These principles included

- strong emphasis on privacy and security;
- an all-of-government approach;
- acceptability to users and fit for purpose;
- opt-in for users;
- an enduring technology-neutral solution; and
- an affordable and reliable solution.

Because of New Zealanders’ strong cultural resistance to government initiatives construed as “Big Brother” activities, such as national ID cards, the government fo-

cused squarely on user centricity, privacy, and security.

New Zealand took an approach that was unique at the time—dividing authentication challenges into logon management and identification. The Authentication Programme’s browser-based logon management is performed via the Government Logon Service (GLS), a pseudonymous identity provider that lets people access many online government services with a single logon. The GLS provides both single and multifactor authentication to support services with different transaction values and associated risks. Identification is performed via the Identity Verification Service (IVS), which makes a verified identity assertion to government agency service providers in a user-controlled manner. This technology uniquely identifies the individual but forwards minimal identity attributes. The tasks of determining user eligibility, role management, and access control are currently outside the Authentication Programme’s scope and remain the responsibility of government agency service providers. The IVS is currently in its initial build stages and will be launched as a limited service with a pilot agency in 2009. The government has confirmed funding for limited service, which will be branded “iGovt.”

The GLS and IVS designs use the Security Assertion Markup Language (SAML), an open standard for communicating security assertions in real time and supported by a growing list of vendor products. Table 1 demonstrates that the use of logically separate key providers enhances the GLS’s privacy by limiting the amount of information any part of the system knows about a specific user. As a pseudonymous identity provider, the GLS delivers a persistent identifier called a federated logon tag (FLT) to a service agency when a user logs on. This FLT is unique to that service user and agency and contains no identity information.

The GLS operates in accordance with SAML’s single-sign-on profile. As Figure 1 shows, when users attempt to access an online service, they’re first redirected to the GLS, where they present a logon key identifier. The GLS passes this logon key identifier to the key provider component for validation against the root key. The key provider component then returns the validated key identifier to the GLS for mapping to the appropriate FLT for

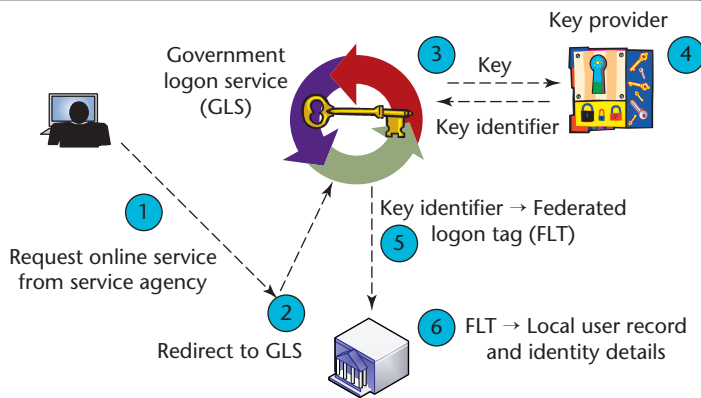


Figure 1. Government Logon Service. The GLS processes shown here depict the actors and message flows that occur when a user logs on to the GLS. The service provider agency receives a federated pseudonymous identifier to attach to customer records in the agency, to recognize the user in future transactions while also preserving privacy and security.

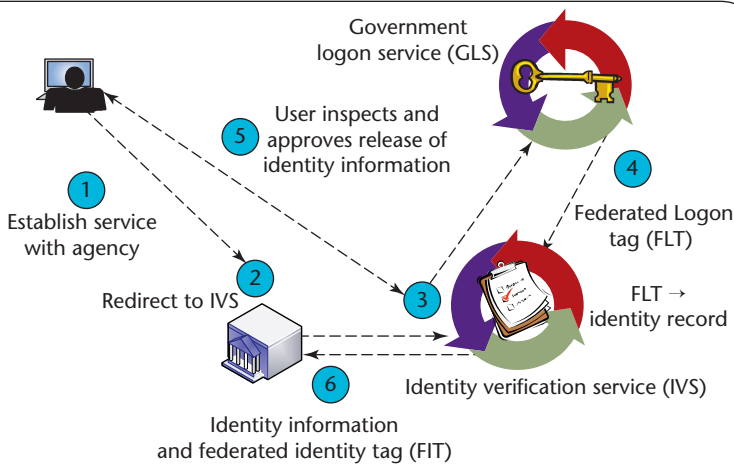


Figure 2. Identity Verification Service. The IVS processes shown here depict the actors and message flows that occur when a user verifies his or her identity to a service provider agency (typically, when users first present themselves to the agency to start a service). The agency receives two federated pseudonymous identifiers, but maintains the user's unique identity

the service provider agency and subsequent passing of the FLT and redirecting the user's browser to the agency. The agency uses the FLT to reference the user in its local store of user information.

The identity assertion that the IVS makes is based on information gained through a standardized proofing process used since 2002 to obtain a New Zealand passport. The IVS also uses SAML and is designed to complement the GLS. Although the IVS can make identity assertions, it has no logon capability—rather, it relies on the GLS to perform logon management and requires users to follow a high-strength logon process to access a service. (Although a high-strength logon typically means using digital certificates, the

New Zealand government has kept its options open in this regard by requiring a two-factor authentication key with at least one hardware token that requires per-session local activation.)

As Figure 2 shows, the IVS starts when users identify themselves to a service provider agency. The agency directs them to the IVS, which redirects them to the GLS for initial logon. After users complete the high-strength logon process, the GLS returns them—and their FLT—to the IVS. The IVS then references each user's verified identity using this tag, and after the user inspects and approves release of his or her identity information, the IVS releases the identity information to the agency along with a federated identity tag (FIT) to attach to the agency's customer record.

From the user's perspective, the IVS and GLS seem to be a single integrated service, but separation of the two services behind the scenes further enhances privacy and makes it impossible for any single party (other than users themselves) to have a comprehensive view of a particular user's interactions with the government.

Service development beyond the GLS and the IVS currently rests on the notion of an Attribute Authority Service (AAS), which will let users request authoritative agencies to make assertions on their behalf—for example, residency status or membership in certain professional groups. After a user authenticates with the GLS, the AAS will display the required information from, say, Agency A and Agency B and, subject to user consent, will send asserted user attributes to the appropriate online service, where the service provider agency will determine eligibility and service access. Aside from system requirements, the AAS won't actually retain the original information in the assertions, which ensures this information is never out of sync with the authoritative source and eliminates the possibility that the service provider agency will use it for some other purpose, potentially reducing the number and nature of data-matching processes required to deliver services.

Comparisons with other jurisdictions

Other countries also use Web-enabled technologies to tackle identity management, often by employing a combination of applications—typically, portals and personal dashboards, national identity schemes, SAML, and the digital certificates and electronic signatures found in public-key infrastructure applications. Table 2 attempts to summarize current and emerging processes in identity management.

Determining the technical details of a wide range of government identity management applications is difficult, so we pulled our information from publicly available material (www.projectliberty.org/liberty/

Table 2. Selected country comparison of technologies used by governments to deliver online services to their citizens.

	PORTAL/DASHBOARD	NATIONAL ID	SAML	DIGITAL CERTIFICATES
Austria	X	X	X	X
Canada	X			X
Catalonia/Spain		X	X	X
Finland		X	X	X
France	X		X	
New Zealand			X	
Netherlands	X	X	X	
Norway	X	X	X	X
UK	X		X	X

resource_center/presentations_webcasts and <http://saml.xml.org/deployments>). We found that several countries, including Norway, Austria, and Spain (specifically, Catalonia), developed their electronic identity management systems based on existing national identity numbers and citizen ID card systems or digital certificate systems. However, these persistent static identifiers could raise the risk of identity fraud or misuse of information when used in an online context, depending on the architectural approach taken and the rigor of the identity establishment/enrollment process. For example, although Austria uses a national-identity-number-based system, it mitigates many privacy risks through the system's technical design, which has distinct similarities to the one New Zealand adopted years later. Austria's source PIN and pseudonymous-sector-specific PIN (ssPIN) authenticates Austrian citizen card holders to a sector agency in a way similar to New Zealand's approach of using a key and FLT. Both approaches display privacy awareness and a strong notion of user control. However, citizen uptake of Austria's system hangs in the balance because the system depends on the complexities of a smartcard, and the market penetration of smartcard readers in Austria remains relatively low.

Austria's system and Catalonia's idCAT Programme have an additional feature: they both use citizen digital certificates for e-signatures to provide for nonrepudiation. The Norwegian government is also considering using digital certificates in this manner—specifically, it's looking at a bank-implemented identity authentication system called BankID as a basis for a government certificate authority. This bucks the trend among European countries to move away from PKI (with the notable exception of Sweden) because they found that using it to deliver government services was difficult for users and expensive to establish and maintain, although some countries still use it in closed group contexts such as the ones in which government employees are involved. The initial extensive use of

digital certificates reflected a widespread awareness of the need for strong security and nonrepudiation, but this technology comes with a history of operational challenges, including complexity and cost. Both factors have affected mass citizen take up (except in Sweden), even though digital certificates can reduce the risk of identity fraud for individuals and government alike in an e-government context (www.schneier.com/paper-pki.pdf).

Another international trend is the use of online portals. They're intended to give users a personal dashboard with greater control over who has access to their credentials, which helps them track their identity usage and makes it easier for them to participate in online services. The Netherlands' Personal Internet Page (<https://www.mijnoverheid.nl>), Norway's MyPage (www.norway.no/minside/), France's Service Public (www.service-public.fr), and the UK's Directgov (www.direct.gov.uk/en/index.htm) are recent examples of a similar approach used some years ago in Canada without much success. The problems in Canada arose when provincial administrations wanted to retain the direct relationship with their users once the centralized authentication process was completed. The administrators were concerned about being perceived as somehow reliant on the federal government for basic functionality. The New Zealand government used the earlier Canadian experience to justify not using its centralized information portal to fulfill its identity management objectives. Agencies are more motivated to get involved because the system design lets them retain relationships with their customers and grants them authorization and access control over their resources. Agencies simply redirect users to the GLS's centralized authentication, which removes any duplicated costs or resources. Because the GLS reduces the number of logons to government agencies that the customer has to manage, the expectation is that citizens will take up more government services online, which, in turn, helps the agencies.

A wide range of reasons help explain the variation in all these approaches, including such factors as different views of what identity management is and what problems need to be solved, the infrastructure or technology available for leverage, the political environment, cost, the time at which identity management solutions are sought or implemented, and the availability of solutions at that time. Against this background, it's also helpful to reflect on the range of approaches to citizen control and risk management.

Cultural, legal, and historical impacts

A key objective in launching an online identity management system is ensuring greater confidence about user identity. But depending on how they implement these initiatives, governments or other parties could have an increased capacity to track unrelated information about individuals with more certainty. For these and other reasons outlined earlier, identity management systems often require high levels of trust in the identity provider—government or otherwise—to be accepted. Not all societies exhibit the same levels of trust in their governments to fulfill this role.

Governments in the UK, US, Canada, New Zealand, and Australia in particular have faced unique challenges in implementing new identity management systems compared with other countries. Citizens are seemingly unwilling to trust government's intentions, with most initiatives attracting strong public scrutiny and demands for greater citizen control and robust privacy measures. In contrast, Scandinavian countries have implemented identity management systems with unique identifiers that don't follow strong privacy, user-control-based models without arousing controversy. Likewise, Singapore and other Asian nations have successfully implemented systems that wouldn't be considered consistent with a strong privacy, user-control-based model.

A key underlying factor in the difference here could be citizens' relationships with their governments: when citizens are confident that their government is trustworthy and has their information under appropriate control, they're less likely to demand direct control over that information themselves. When citizens are less sure about government's trustworthiness, and they're concerned that private information in government hands could be misused, used for unrelated purposes, or not properly protected, they might be more likely to demand direct citizen control over identity management. In Scandinavian countries, for example, our experience has been that people have higher levels of trust in government than in the US, UK, Australia, or New Zealand, perhaps because Scandinavian governments have a different

framework for trustworthiness. Their centuries of government openness, including freedom of information laws, appear to have contributed to citizens showing higher levels of comfort about how their information will be handled (<http://aitel.hist.no/~walterk/wkeim/foil.htm#liste>). Trust in government and the way it handles private information might be less of an issue in the uptake of a new identity management system when the government has a historic tradition of strong central authority.

Implications for identity management

When citizen uncertainty about government trustworthiness is an issue, approaches to identity management that factor in user control and user-centric approaches to risk are more likely to achieve community acceptance.

As we've mentioned, the risk associated with online identity management is sometimes unfairly shifted to the citizen, who isn't always in a good position to bear it and might not be willing to do so. This shifting of risk can take several forms. For example, the citizen might

- suffer financial loss by interacting with a fraudulent entity;
- experience major life disruption through the loss of identity credentials or fraudulent misuse of those credentials;
- be unfairly discriminated against by inappropriate secondary use of data trails left in the identity management system; or
- bear the burden of dealing with these failures, including attempting to gain redress and returning life to normal.

To counter these problems, several mechanisms give appropriate levels of user control and help manage risk, but none of them are likely to be sufficient on their own. The type of organization and the nature of the technology used and how it's deployed are important in deciding the right mix. Other key factors include

- education about the risks involved in an identity management system;
- law as a way for government to make promises to protect citizens and back up those promises; and
- technology as a way of designing in security, risk, and control mechanisms.

Clearly, education, law, and technology on their own aren't enough to have a major impact on citizen privacy and life control—it also requires mechanisms that can demonstrate that the measures in place are

actually effective. Good governance is essential to ensure that an organization spells out clearly what it will do in terms of control and allocation of risk, and very importantly, to prove that it does what it said it would do. Governance mechanisms should start with internal management metrics and feedback and extend to outward-facing mechanisms, such as reports to ministers, external audits, regulators, and any other continuous disclosure obligations. In particular circumstances, they can extend even further, to investigation and enforcement action.

Although many organizations anticipate and plan for inevitable failures and incorporate responsive mechanisms, such as the business continuity plans, it's just as important to provide the equivalent for the individual—in effect, to create a citizen continuity plan. Failures will happen regardless of the quality of the education, legal, technological, or governance arrangements in place: these arrangements minimize the chance of failure but don't eliminate it; thus, a good safety net is essential. It should include accessible, individual responses for when things go wrong. Lack of a good safety net is tantamount to allocating a disproportionate amount of risk to the individual, who is often least able to manage, mitigate, or bear that risk compared with the service provider.

Beyond their immediate territorial boundaries, governments must also consider the extent to which they accept other governments' identity credentials and the basis on which they do so. In fact, they might have to be more flexible in the approach they take to other credentials than in developing their own.

Our brief survey revealed that governments use different technologies to implement their identity management strategies, and we found that their approaches depended on a range of factors, including the cultural, legal, and historical ones introduced here. Our first-hand experience with the effects of historical and cultural differences on concerted attempts to create a single international identity management standard suggests that pursuing a single standard for identity management presents a significant challenge.

The New Zealand example demonstrates the value of starting from a sound understanding of the policy environment and a clear vision of what is to be achieved. The citizen response to the New Zealand approach is yet to be revealed, but because the approach focuses clearly on user control, unimpeded by national security and law enforcement objectives, it might be able to avoid the trap of citizen rejection experienced by other governments attempting to combine such objectives into a single identity management approach. E-government and its connection with identity management

are still too immature to conclusively say that one approach is better than another. Whatever approach is adopted, its ultimate success will be judged by citizen acceptance—or the ballot box, a rather slow and blunt instrument. The key factors are the quality and depth of citizen engagement with (or disengagement from) government and the extent to which citizens adopt Web 2.0 values and strategies to bypass government services if they aren't satisfied about privacy and security.

This is a rapidly developing debate, and there are several ways you can contribute to it. Standards development organizations such as Liberty Alliance and Oasis are eager for more use cases on which to develop further specifications—for example, the recent expansion of identity selectors available to users could ultimately pressure existing government identity management applications to be able to interact more fluidly. They could also pressure vendors to move beyond interoperability to the much more challenging goal of convergence. You can find further discussion on such topics at www.theconnect-edrepublic.org/blog/, www.idcorner.org, and www.identityblog.com. □

References

1. S. Pruitt, "Microsoft Ordered to Fix Passport Problems," *PC World*, 8 Aug. 2002; www.pcworld.com/article/id,103712/article.html.
2. A. McCue, "ID Card Support Collapses," *silicon.com*, 13 Mar. 2006; www.silicon.com/publicsector/0,3800010403,39157146,00.htm.

Robin McKenzie is a principal consultant at Information Integrity Solutions. Her expertise includes privacy and identity management, e-government and Web 2.0, and privacy impact assessment. McKenzie has a law degree from the University of Adelaide and an honors arts degree in social anthropology from Monash University in Melbourne. Contact her at rmckenzie@iispartners.com.

Malcolm Crompton is managing director at Information Integrity Solutions. His expertise is in the areas of identity management, e-government, Web 2.0, and privacy impact assessment. Crompton was Privacy Commissioner of Australia from 1999 to 2004. In 2004, he received the Inaugural Chancellor's Medal for distinguished contribution to the Australian National University. Contact him at mcrompton@iispartners.com.

Colin Wallis is the program manager of authentication standards for the New Zealand government's all-of-government Authentication Programme. He also serves as chair of the e-government special interest group for the Liberty Alliance Project. Wallis has a commerce degree from the University of Otago, Dunedin, New Zealand. Contact him on colin.wallis@ssc.govt.nz.