

2007
IDDY
AWARD
WINNER

Case Study:

New Zealand Sets the Pace for SAML 2.0 Deployments

New Zealand proves that great things often come from small countries as it joins the ranks of e-government SAML 2.0 deployers with its wide-ranging all-of-government authentication program.

This innovative program is committed to providing shared services based on the principles of federated user-centric Identity Management—security, privacy and user control—and promises to transform how government relates to citizens and business.

“Our goal is to raise the level of citizen participation and engagement with government via the online channel,” said Colin Wallis, the Authentication Standards Programme Manager at the State Services Commission, the agency in charge of New Zealand’s e-government projects. “Liberty Alliance has been instrumental in helping us achieve that goal.”



Simplifying E-access for Citizens

New Zealand, with about 4 million citizens, maintains approximately 35 central (federal) public service departments and another 70 agencies outside the central (federal) sphere. Increasingly, citizens were forced to log in to different agencies individually. And in this environment, there was the prospect that an individual might have 15–20 passwords and authentication devices in order to interact with various government functions.

“With a proliferation of agencies and Web sites with transaction services, we were facing a situation of password overload and increasing security risk,” said Colin. “We really needed to find a way to authenticate individuals with security, privacy and the user experience in mind.”

In 2000, the New Zealand All-of-government Authentication Program (<http://www.e.govt.nz/services/authentication>) was formally launched with the aim of

“In order to participate, agencies are naturally going to ask: What products should we use? And the short answer is: Use Liberty conformant products. We point them to the Liberty Web site and the conformance page and say: This is your choice of products—some products will do things that others won’t, depending on your needs, but it is not in the public interest to spend more time and money integrating a product that’s not Liberty conformant. It’s very simple.”

Colin Wallis

The Authentication Standards Programme Manager at the State Services Commission, the agency in charge of New Zealand’s e-government projects.

determining what the government could do to help New Zealand citizens and businesses more conveniently and securely authenticate themselves when transacting with government agencies using the Internet.

New Zealand wanted to make it much easier for citizens to engage with the government online and find a solution that would ultimately support single sign-on. They also wanted citizens to be able to give the government a piece of information once and, with their consent, allow that information to be reused by citizens across government and not be given time and time again.

The policy team also identified a set of contextual factors that had to be addressed in order to build a successful solution. These factors included:

- Strong emphasis on compliance with Privacy legislation
- Cultural resistance to any national identifier or ID card
- Low national security and illegal immigration drivers
- Inter-agency data matching prohibited except by (a small number of) specific exceptions
- Citizen consent to and control of use/release of data
- Opt-in for citizens: not compelled to use the services
- Shared services that could scale to meet the needs of all government agencies
- Low risk, low budget approach with controlled steps forward

Although government agency use cases are the foundation of the project, Wallis also emphasized the importance of buy-in from everyone who would be potentially impacted, including users, government service agencies, vendors, and key standards organizations—including Liberty. “A project like this doesn’t happen in a vacuum,” said Wallis. “Everyone has to own part of the outcome. We felt it was important to have the stakeholders focused on the user experience, not on each other.”

Structuring Identity-based Solutions

After much research and review of cultural and policy considerations, New Zealand opted to develop two centralized shared services: an Authentication Service (Government Logon Service—GLS) and a separate Identity Verification Service (IVS). (The GLS and IVS are internal “working names” for these services during the course of the branding and marketing process.) The management of Authorization, frequently associated with Authentication and Identity Management, remains the responsibility of government agencies.

Starting in 2004, the GLS was developed first, using SAML 1.x (remember that SAML 2.0 was not yet released back then). This service offers agencies that connect to it persistent pseudonymous identifiers to protect user privacy and multifactor authentication methods for added security where the agency’s risk assessment points to the need for such protection.

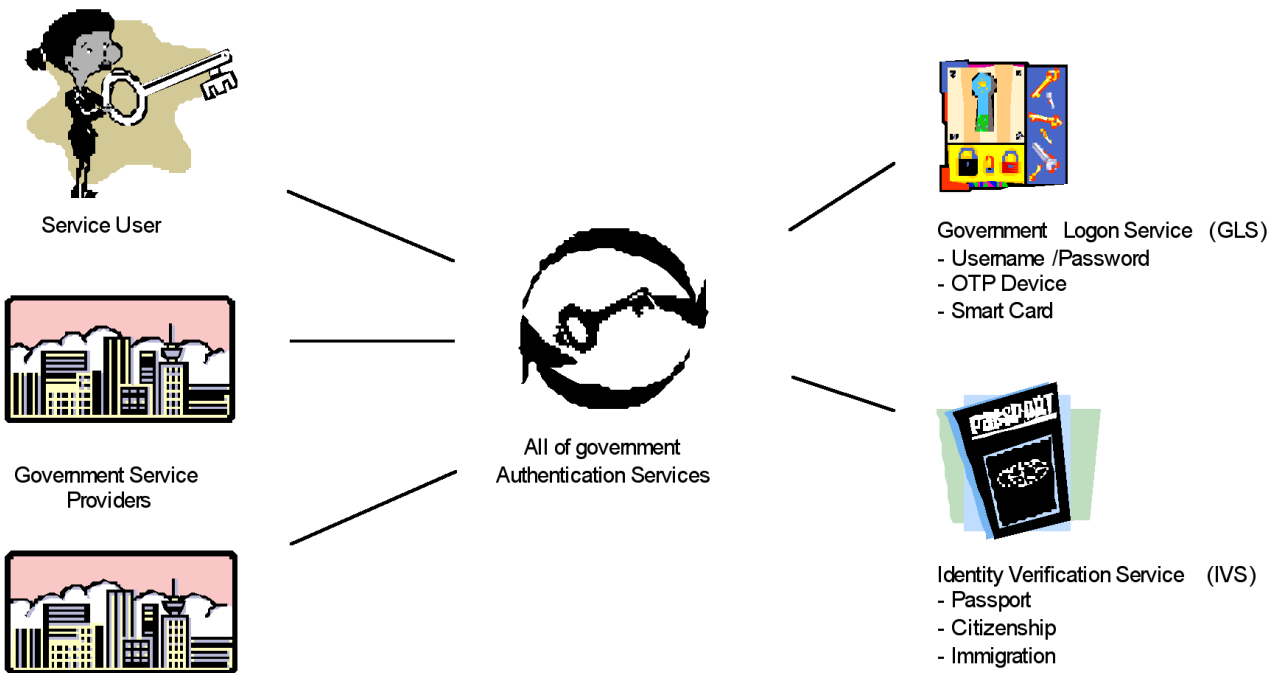


Figure 1: A conceptual overview of the New Zealand government's Identity Management implementation.

In design right now is an Identity Verification Service where the user can choose to have their verified core identity attributes electronically stored in a centralized database. Citizens can log on to the centralized IVS via the GLS and release their identity attributes (real or pseudonymous) to other agencies they wish to receive service from, versus having to prove identity to multiple departments. This approach offers more user control over the access to, release to, and use of PII by the agency.

Each agency receives its own unique persistent identifier for the person along with the person's identity attributes. By ensuring that no single national identifier is used by agencies this way, privacy protection is "designed into" the system.

Developing the Notion of Attribute Authorities

"It's clear that the architectural approach supports the notion of multiple identity providers. But for reasons of cost and expertise overlap, we want to limit the duplication of the government's investment in

verifying and maintaining identity data across agencies. The greater the amount of duplication, the bigger the issue of security and privacy in terms of appropriate use of the information—using the most up-to-date information and so on,” said Wallis. “Instead, we are garnering support for the idea that different agencies act as sources of other types of information—information held in government registers by agencies considered to be authoritative in their domain.”

The idea of the Attribute Authority Service will allow a user to request that the authoritative agency make an assertion on their behalf. Among the many possible types of assertions the government could make on a person’s behalf include: directorship of a company, residency status or membership in certain professional groups.

The basic use case of the Attribute Authority Service involves a citizen who wants to use an online government service. This service requires the user to provide certain information from Agency A and Agency B to determine their eligibility. Instead of requiring traditional paper documentation, the online service allows the user the option of requesting Agencies A and B to make a real-time attribute assertion to fulfill the requirement. After the user authenticates at the GLS, the required information from Agency A and Agency B is displayed to the user and, subject to user consent, is sent to the online service where eligibility and service access is determined. Notwithstanding auditing and logging requirements, the

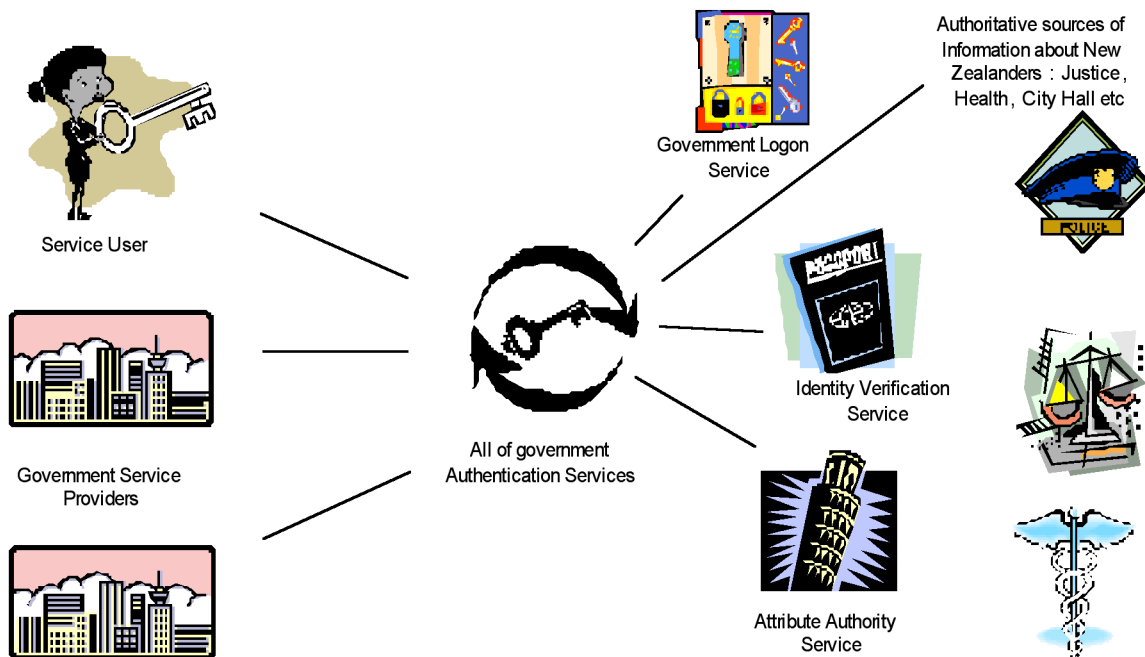


Figure 2: A conceptual overview of the Identity Management system developed to include the notion of the Attribute Authority Service.

Attribute Authority Service does not actually retain the information in the assertions—thereby ensuring the information is never out of sync with the authoritative source and eliminating the possibility that it will be used for some other purpose. It's a classic melding of security supporting privacy.

User centric control is the single most important feature of this model. Users must initiate and approve any information sent from the authoritative agency.

The approach also has a beneficial effect on reducing the number and nature of data matching processes required—in New Zealand these require parliamentary approval. These can be limited to law enforcement requirements and do not compromise the integrity of the customer-centric IdM solution.

Enter Liberty Alliance

In order to deploy identity effectively and securely, it was clear from the beginning that standards were critical. "You need standards right from identity proofing, through authentication, authorization and federation," said Wallis. "We started with the existing open standards and other (primarily U.S. government) standards and then 'cook booked' them together to support an integrated Identity Management system."

In 2005, New Zealand began to develop its own deployment profile of SAML 2.0 by "observing" on the OASIS Security Services Technical Committee. As vendor product conformance became more critical to implementing the SAML 2.0 deployment profile, the New Zealand program became drawn into the work that Liberty was doing, and the State Service Commission joined Liberty in 2006. Subsequently, as the future direction of the program became clearer and New Zealand's Identity Management use cases were becoming increasingly complex, interest turned to Liberty's Web services-based specifications that extended and complemented the simpler browser-based messaging for SAML 2.0.

"Liberty was integrating SAML into Web services and building the useful, practical profiles, so we turned to Liberty for direction," said Wallis.

According to Wallis, the engagement with Liberty Alliance has been immensely rewarding, and is one of the few spaces where vendors and users can talk openly to each other about customer requirements and the vendor community's capability to fulfill them—without the pressure to make a sale. Liberty with all its resources, including multiple special interest groups (SIGs), cut to the deployment chase.

New Zealand E-Government Goals

By **2007**, information and communication technologies will be integral to the delivery of government information, services and processes.

By **2010**, the operation of government will be transformed as government agencies and their partners use technology to provide user-centered information and services and achieve joint outcomes.

By **2020**, people's engagement with the government will have been **transformed**, as increasing and innovative use is made of the opportunities offered by network technologies.

“One of the biggest problems the governments face in dealing with vendors is as soon as you have a meeting with one, the others say, ‘Why weren’t we invited?’” said Wallis. “And if you get them all in a room together they typically don’t say anything because they are frightened of giving away competitive advantage. The idea that there’s a place like Liberty where it’s a level playing field for vendors and users to come together without any pretensions or expectations was extremely attractive to us.”

“The drive towards federated identity has been largely vendor driven because it’s taken a while for customers to catch on. But as we do, and we come to know our requirements, vendors in Liberty are keen to listen, with a view to modify their offerings accordingly,” Wallis added.

The Concordia initiative has taken this aspect of the organization’s strategy to a new level. “As the IdM space became more defined in 2006, the private sector and government members became more vocal about the need for applications to support multiple single sign-on technologies that may be in the hands of the end users. It is a credit to those who had the most to lose, to embrace this initiative and to try to sidestep repeating the problems of the past,” said Wallis.

Another major benefit from the Alliance, says Wallis, is the non-technical and policy efforts. “When we joined, we were not aware that Liberty was starting work on those real thorny legal issues around establishing Circles of Trust and framing liability. The value coming from these has been a welcome and unexpected bonus,” he said.

Liberty Conformance Testing Speeds Deployment

Wallis pointed to the critical role that Liberty’s conformance testing program plays, ensuring that different vendor products will interoperate.

“The conformance program was probably the single most important thing that Liberty offered us,” said Wallis. “We didn’t have the funds to mount a separate interop testing program like the U.S. government,

Liberty Interoperable™

The Liberty Alliance’s Liberty Interoperable™ program was created with the goal of providing product and application vendors a confidential environment in which to test their products against Liberty’s standards and specifications. Liberty has certified over 75 solutions from numerous vendors and organizations worldwide.

The success of the program is demonstrated by the wide scale deployment of Liberty Interoperable products and by the increasing number of RFPs issued around the world that require vendors to have passed Liberty Alliance testing. We needed to find ways to scale the program to meet new growth and interoperability demands, especially now that ID-WSF 2.0 is final and works seamlessly with SAML 2.0.

For more information on the Liberty Interoperable program go to:http://www.projectliberty.org/index.php/liberty/liberty_interoperable

but armed with our own profile as well as Liberty's conformance program we have the basis of something to work with. It facilitates the entire deployment process and speeds time to market for everyone.

"In order to participate, agencies are naturally going to ask: What products should we use? And the short answer is: Use Liberty conformant products. We point them to the Liberty Web site and the conformance page and say: This is your choice of products—some products will do things that others won't, depending on your needs, but it is not in the public interest to spend more time and money integrating a product that's not Liberty conformant. It's very simple."

"As more governments adopt SAML 2.0 (the U.S., Denmark, and NZ government profiles are available amongst others), there is a great opportunity for us all to develop an agreed 'government profile' for the vendor community. It's a huge challenge, but just imagine the turbo boost to the deployment rate!" he added.

Reviewing and Assessing: Lessons Learned

Wallis points to 10 lessons learned from their identity management deployment experience so far:

- Carry out a risk assessment on your service as soon as possible so you know what problems need resolving.
- Engage the standards and specifications organizations early and be proactive in defining your requirements.
- Use subject matter experts found in standards and specifications organizations to map your requirements and identify gaps.
- Establish stronger links between the organizations, the subject matter experts, and the program of work with the local vendor community during development. This will help knowledge transfer and drive a consistent approach.
- Be mindful of your organization's procurement rules and policies when engaging vendor assistance on your early development.
- Profile everything to limit the options according to your requirements and drive a consistent approach—a standard is not an instruction manual.
- "Design-in" privacy and security—do not layer it over the top—if you want to pass public scrutiny and privacy impact assessments!
- Don't mix identity management with law enforcement management—keep them separate and deal with them appropriately and transparently if you want to maintain customer confidence and trust.
- Pretty much anything can be resolved on the technical front. The hardest part of Identity Management is implementing the business process and legal aspects.
- Understand the changing nature of your relationship with standards and specifications organizations—to begin with, you depend on them; as you mature, it becomes more of a partnership. As time goes on, expect your involvement to increase, not reduce.

Looking to the Future: Summary of Trends and Action Points for New Zealand Agencies

The Death of Passwords

There was a sense that 2006 was, finally, the tipping point for the demise of passwords for online services that have moderate or high security requirements. There are now viable alternatives with two-factor authentication solutions spanning a wide range of price points, form factors, and strengths.

Action Point for Agencies: Conduct a high-quality risk assessment of online services and, where the risks are found to be moderate or high, an introduction of an appropriate two-factor authentication solution is recommended.

Identity's Third Wave: User-centric Identity

In the past year, the Third Wave of Identity has developed into a full-fledged wave. The characteristics of this user-centric identity framework includes user control, consistent experience across Web sites, protection of privacy, interoperability, multiple roles for people, multiple identity/attribute providers, and increased security.

Action Point for Agencies: Agencies need to consider what the paradigm-shifting nature of user-centric identity means for them and respond. The future framework puts service users at the center, using online services from multiple agencies and in control of the authentication exchange.

Old Scams, New Channel

In the past year or so, organized crime mobs have cemented their domination of the global cybercrime industry. As the New Zealand government steps up using the Internet and provides online services that have greater financial and reputational risks, it is inevitable that it will attract the attention of the Internet Mafia.

Action Point for Agencies: Agencies need to work collectively to tackle this menace and maintain people's trust in the online channel at all-of-government and all-of-New Zealand levels.

Authentication Is Not Just Identity Alone

The move towards user-centric identity and the rise of Web 2.0 has given rise to a trend for verifying information about a person online beyond just unique identity. For agencies there are many times when it is important to know a person's attributes authoritatively and online (in addition to the identity of the person uniquely).

Action Point for Agencies: Agencies should widen their understanding of authentication to be the online, real-time verification of a person's or organization's attributes, typically used for determining authorization and/or entitlement, and not unique identity alone.

Authentication Gets Dynamic

A trend is emerging with some service providers taking an approach that the risk from people accessing online services from their normal computer should only require a low strength of authentication. They therefore advocate that the type (strength) of authentication required should be dynamic rather than the same across the board.

Action Point for Agencies: For agencies considering dynamic authentication, caution is advised until this approach proves itself. On the other hand, if and once it does, dynamic authentication may be a useful addition as a part of a wider, integrated suite of authentication services.

SAML 2.0: the Default Choice

All three of the major open standards for identity federation have come together in Security Assertion Markup Language (SAML) v2.0. Over the past year, there have been several commercial off-the-shelf and open standards software products introduced.

Action Point for Agencies: When developing or re-developing identity management systems, agencies should consider SAML 2.0 as the default choice in implementing identity management messaging online.

About Liberty Alliance

Liberty Alliance is the only global identity organization with a membership base that includes technology vendors, consumer service providers and educational and government organizations working together to build a more trusted Internet by addressing the technology, business and privacy aspects of digital identity management. The Liberty Alliance Management Board consists of representatives from AOL, Ericsson, Fidelity Investments, France Telecom, HP, Intel, Novell, NTT, Oracle, and Sun Microsystems. Liberty Alliance works with identity organizations worldwide to ensure all voices are included in the global identity discussion and regularly holds and participates in public events designed to advance the harmonization and interoperability of CardSpace, Liberty Federation (SAML 2.0), Liberty Web Services, OpenID and WS-* specifications. More information about Liberty Alliance as well as information about how to join many of its public groups and mail lists is available at **www.projectliberty.org**