The Liberty Alliance

GLOBAL ADOPTION

NEWSLETTER

Volume VI
Fall 2007

FOCUS on E-GOVERNMENT

www.projectliberty.org

LIBERTY ALLIANCE

LIBERTY ALLIANCE GLOBAL ADOPTION NEWSLETTER

CONTENTS

LIBERTY ALLIANCE

New Initiatives:

Interoperability Workshop Series, Identity Assurance Expert Group Formation

Liberty E-Gov Interoperability Workshop: First of a Series of Market-Specific Workshops Focused on Driving Interoperability

Attention all SAML 2.0 deployers, vendors and anyone with an interest in identity management interoperability between e-government deployments worldwide. Liberty Alliance is pleased to announce a face-to-face Interoperability Workshop September 19—21, 2007, in Piscataway, NJ, USA. This is the first of a series of interoperability workshops focused on specific vertical market deployment profiles of Liberty Federations (SAML 2.0) and Liberty Web Services (ID-WSF). The first workshop will provide implementers (both product vendors and credential service providers) a chance to learn more about the GSA eAuthentication Solution deployment profile for SAML 2.0 before the Liberty Alliance Interoperable™ certification against that profile begins October 1st.

Please note that SAML 2.0 is the defacto standard for federated identity solutions in many governments and this workshop will feature a second working track focused on harmonizing the e-government deployment profiles of SAML 2.0 across many governments including representative government participants from Asia/Pacific and Europe. There is no required relation between this optional workshop and the October 1 certification event, and participants may register for one or the other independently.

This is an excellent opportunity to test GSA-compliant SAML 2.0 implementations in a collegial, confidential environment. The event is particularly relevant to implementation developers, implementation QA/testers and pre-sales or deployment engineers. This event is open to Liberty members and non-members alike.

For more info and registration:
http://www.projectliberty.org/news_events/events/saml_2_0_face_to_face_interoperability_workshop

Liberty Establishes the Identity Assurance Expert Group

Liberty has formed a new global expert group to deliver the Liberty Trust Framework, an organizational framework designed to fill industry requirements for standardized identity assurance criteria for use in a broad range of federation scenarios.

Liberty's Identity Assurance Expert Group (IAEG) was established by the recent merge of the Electronic Authentication Partnership (EAP) into Liberty Alliance, and consists of representatives from the global financial services, government, healthcare and service provider sectors working collaboratively to release the Liberty Trust Framework for public review and input later this year. The new group is co-chaired by Jane Hennessy, Senior Vice President, Wells Fargo Bank, N.A., and Michael Sessa, Executive Director, Postsecondary Electronic Standards Council (PESC).

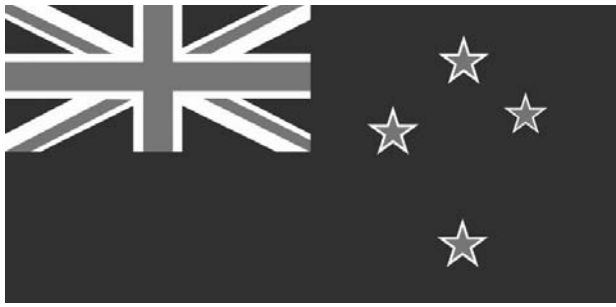
The Liberty Trust Framework will remove a major barrier to global inter-federation deployments: the complexity of assessing the level of identity assurance among all organizations participating in federated relationships. Currently, different federations have varying policies and processes governing identity operations, the interpretation of which adds to the cost and complexity of deploying assured identity services. The Liberty Trust Framework will provide a standard set of criteria so that identity transactions, with assurance requirements ranging from leaving a comment on a blog to high-value financial transactions, can move ahead based on a standard framework for managing identity assurance levels and associated business processes and technologies. With common criteria for determining accurate identities in place, the Liberty Trust Framework will make it easier to bring new members into existing federations as well as simplify how federations themselves can interoperate.

Initial major contributions to the Liberty Trust Framework are coming from the Trust Framework of the EAP and the Credential Assessment Framework of the US E-Authentication Federation. Liberty Alliance acknowledges the importance of these contributions in allowing the IAEG to rapidly create the Liberty Trust Framework. The Framework will be defined in a way that scales, empowers business processes, and benefits individual users of identity assurance services among federations potentially supporting billions of simultaneous transactions across devices, industries and regions.

For more information go to:
http://www.projectliberty.org/liberty/strategic_initiatives/electronic_id_assurance
or contact: brett@projectliberty.org

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 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.

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.

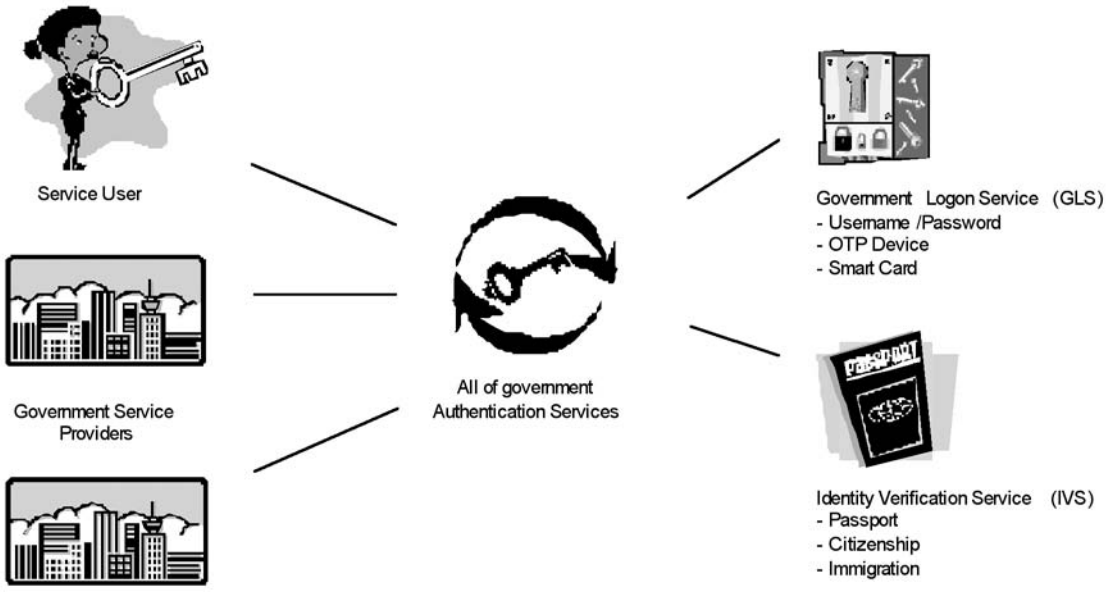


Figure 1: A conceptual overview of the New Zealand government's Identity Management implementation.

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 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.

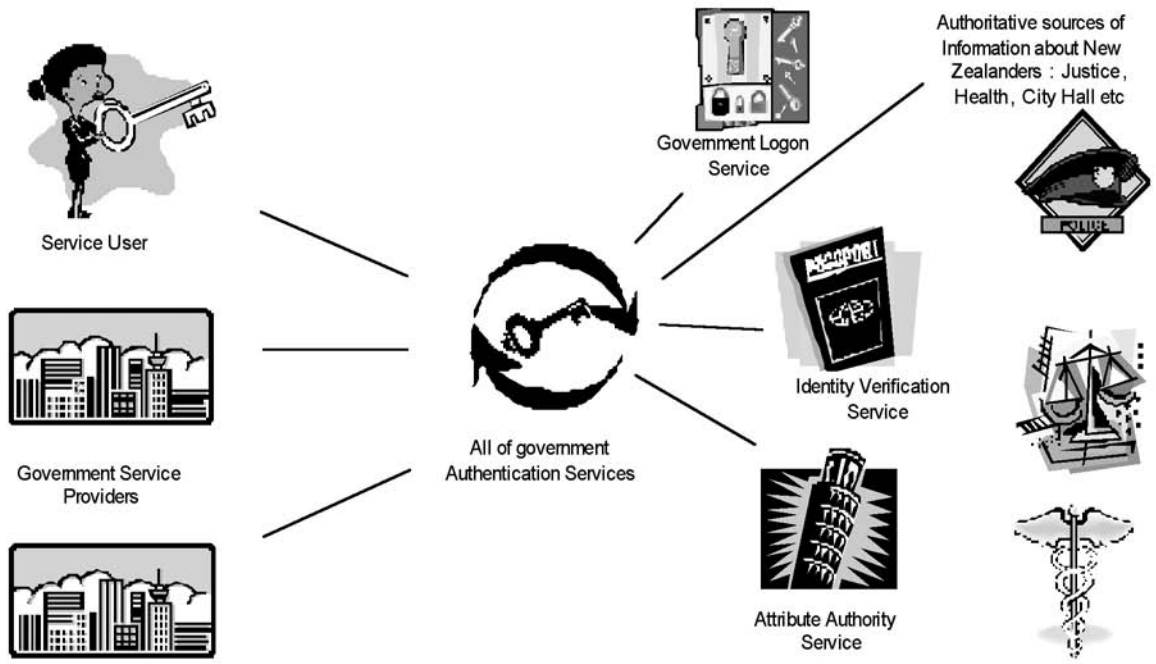


Figure 2: A conceptual overview of the Identity Management system developed to include the notion of the Attribute Authority Service

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.

"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, 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.

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.

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

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.

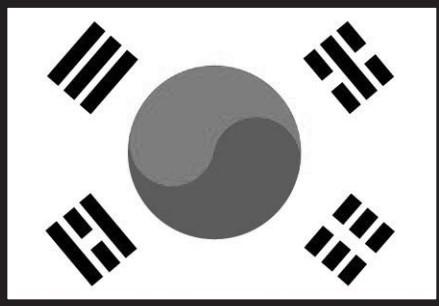
Action Point for Agencies: For agencies considering dynamic authentication, caution is advised until this approach proves itself. On the other hand, if and once it does, dynamic authentication may be a useful addition as a part of a wider, integrated suite of authentication services.

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.

Boy Band Promotes South Korean E-Government



In what might be the most innovative e-government marketing move of the year, South Korea is using a celebrity boy band to promote their new e-government implementation.

Members of the band, DBSK (Dong Bang Shin Ki), are serving as e-government ambassadors and appearing throughout South Korea talking about the benefits of the new solution.

DBSK

Most of DBSK's music is mainstream K-pop (Korean popular music). The band often wears stylized outfits and perform choreographed dance moves. Their name translates into "Gods Rising from the East."

At a recent ceremony, the Minister of Government Administration formally named and honored the band members as Ambassadors. The band's leader demonstrated how to use the e-government services and said, "Administrative services used to involve a lot of manual work. It used to be very complicated. The e-government system has solved those problems and the online system is very user friendly."

He asked the crowd to show "encouragement for e-government and encouragement for his band."

South Korea deploys Liberty federation in ETRI, their Integrated Identity Management Services.

To watch a video of the announcement go to:
http://www.youtube.com/watch?v=kSiupkONuNM

Understanding the Identity Governance Framework

Over the past several months, there has been a lot of buzz around the Identity Governance Framework (IGF). Naturally, Liberty members, the media and others have been asking what does it offer? What are its goals? What is Liberty Alliance's unique role?

The IGF is an open standards-based initiative developed to help organizations better govern and protect sensitive identity-related employee, customer and partner information as it flows across heterogeneous applications. It establishes a standard way of defining enterprise-level policies for organizations to share sensitive personal information securely and confidently between applications and diverse identity sources while helping ensure security and privacy. With the IGF, organizations can more easily determine and control how identity information—including personally identifiable information, access entitlements and personal attributes—is used, stored and propagated across diverse systems, helping ensure the information is easily auditable and not abused, compromised or misplaced.

History

Oracle released a draft of the IGF in Nov. 2006 with industry support for the initiative from CA, HP, Layer 7, Novell, Ping Identity, Securent and Sun Microsystems.In February, Oracle submitted the Identity Governance Framework (IGF) royalty-free to Liberty Alliance. Liberty Alliance has been leveraging its expert groups, diverse global membership and leadership in addressing the technology, business and privacy aspects of digital identity management to further develop the IGF specifications.

The further development of the IGF within Liberty Alliance has been based on the Liberty model of creating open and secure identity standards, business and policy deployment guidelines and best practices for managing privacy in a collaborative environment where all members are invited to participate. This approach, where standards are developed only after well-defined use cases are in place, helps to ensure that the output of Liberty Alliance meets business and user requirements for interoperable, secure and privacy-respecting digital identity management solutions.

"Since its launch, vendors and customers alike have expressed enthusiasm for the IGF and view it as an effective means for better managing and protecting identity information across the extended enterprise," said Hasan Rizvi, vice president of Identity Management and Security Products, Oracle. "Liberty's membership—spanning vendors and customers—has significant experience in addressing the technology, business and privacy aspects of identity. Their success in driving open and secure identity standards made the consortium a natural choice for advancing the IGF specifications."

Prateek Mishra chaired the IGF MRD work, leading a group of Liberty Alliance members working within Liberty's Business and Marketing Expert Group to develop the scope-of-work and market requirement documentation to further advance the IGF. The team completed the MRD in June 2007, and it is now published for public review at http://www.projectliberty.org/index.php/liberty/content/download/3432/22922/file/Liberty_Id_Governance_mrd-v1.0.pdf

Frequently Asked Questions About the IGF

Why is a new approach needed?

The governance and protection of sensitive personal information of employees, customers, and partners as it flows through IT systems is increasingly mandated by privacy and compliance regulations. However, to date there has been no easy way to enforce these controls across the

typical heterogeneous IT environments. As a result, identity-related data (personal identifiable information, entitlements, attributes, etc.) is sometimes scattered across numerous applications within an organization, making such information prone to inconsistencies and even placing it at risk. Alternatively, such information may be so strictly controlled that applications that could benefit from it are prevented from doing so.

Additionally, the number of protocols proposed with which to transfer identity-related data are growing. While each protocol might define protocol-specific ways with which to protect information, we must consider that data being transferred in a multi-protocol environment must be handled consistently. Therefore policy between protocols needs to either follow the same open standard, or be easily mapped and convertible.

Organizations need a standards-based solution that helps define policies, enforce controls, and track activities pertaining to usage of identity-related data. Identity Governance Framework (IGF) will help enterprises easily determine and enforce how identity-related information (including Personally Identifiable Information (PII), entitlements, attributes, etc.) is used, stored, and propagated between their systems. IGF will enable organizations to define enterprise level policies to securely and confidently share sensitive personal information between applications that need such, without having to compromise on business agility or efficiency.

What about Liberty Alliance/SAML? Haven't these problems already been solved by those frameworks?

To date, there has been extensive work by Liberty and other standards groups, like OASIS, on browser-based or user-centric identity. IGF's goal is to complement those efforts. IGF focuses on the data exchanges and interactions that occur behind Web sites. An example might be a travel booking service communicating with the airline to book travel on the user's behalf. The objective of IGF is to take the next step and provide a governance framework for the use, storage, and exchange of identity-related data in a services-oriented-identity or "SOI" approach.

What about Higgins, Bandit, CardSpace or WS-Trust? Don't they address this problem?

Efforts such as Higgins, Bandit, and CardSpace are focused on user-centric identity privacy. They are primarily designed to empower end-users to control how information about themselves is shared with various service providers. They do not address the issues of policy and obligation of identity-related data between enterprise systems not directly exposed to the end-user. Identity Governance Framework is designed to complement and co-exist with these efforts. Higgins/Bandit also have a data access component called IdAs. It is conceivable that IdAs could be adapted to be used as the data connector and modeling components for IGF's policy and service provider layers in an open source implementation. In this case, IdAs is a choice that could be made by an implementer of the IGF framework.

What about WS-Policy? Doesn't it address all of these different policy issues?

WS-Policy is a draft specification currently under development within the W3C. It provides "containers" that can carry different types of "service meta-data" and enables policy matching and selection from alternatives. The underlying service meta-data is drawn from specific domains such as security, reliability or other service properties such as identity, and fall beyond the scope of the WS-Policy specification. The first working drafts of the specification have recently been published in November 2006. The next revisions of the CARML and AAPML drafts will appropriately reference these drafts. These will likely document how CARML/AAPML can be embedded or mapped to a WS-Policy.

How will IGF benefit customers?

Organizations are burdened with protecting sensitive personal information about their customers, employees, and partners. Data regarding social security numbers, credit card numbers, medical history and more are increasingly under scrutiny by regulations seeking to

prevent abuse or theft of such information. To date, privacy conscious organizations have reacted to these requirements by enforcing overly strict controls and processes that hinder business operations and impact productivity, flexibility, and efficiency. At the opposite end of the spectrum, some organizations do not take the care needed to safeguard this information, potentially putting identity-related data at risk without sufficient oversight and control.

The Identity Governance Framework will enable a standards-based mechanism for enterprises to establish "contracts" between their applications such that identity-related information (including Personally Identifiable Information, entitlements, attributes, etc.) can be shared securely with the confidence that this data will not be abused, compromised, or misplaced. Using this framework, organizations will have complete visibility into how identity information is stored, used, and propagated throughout their business. They'll be able to automate controls to streamline business processes without fear of compromising the confidentiality of sensitive identity-related information.

How will IGF benefit ISVs?

Independent Software Vendors developing business applications packages will be able to easily meet their customers' requirements for secure and auditable usage of identity-related data. By writing to the IGF specifications and framework they will be able to leverage existing technologies and methodologies, while at the same time making their products interoperable out-of-the-box with other third-party products.

How will IGF benefit service providers?

External or outsourced service providers (e.g., corporate procurement, business travel, HR, and payroll) who require and use identity-related data will now be able to provide documentation and audited use of identity information, making it possible for corporate clients to act as identity providers to ASPs. Together with federation technologies such as WS-Trust, and SAML, service providers will now also be able to

trust attribute information from identity providers directly without having to copy and replicate information, thereby opening them up to increased risk exposure.

How will IGF benefit developers?

The Identity Governance Framework will yield an industry agreed-upon method for how identity-related data is treated when writing applications. This will provide developers a standards-based way to easily write applications that use this data so that governing policies can be used to control it. This will result in faster application development times as well as guarantees of future compatibility for applications that are written to the eventual standards. Specifically, use of the CARML API will enable developers to defer deciding on how identity-related information will be stored and accessed by their application.

Developers will not need to worry about whether they should use a SQL database, LDAP Directory, or other system. In the past, developers were forced to write highly specific code, driving technology and vendor lock-in. By using CARML declaration, applications will be able to support flexible deployment into a wide range of environments without the need for ongoing specialized developer enhancements. The IGF Attribute Service will do all the hard work of data retrieval, transformation, and policy enforcement when it comes to identity-based information.

What is the Identity Governance Framework comprised of?

The major components of the Identity Governance Framework include:

- Client Attribute Requirement Markup Language (CARML – pronounced car-mull) – a declarative contract document defined by application developers that informs deployment managers and service providers of the attribute usage requirements of an application.

- Attribute Authority Policy Markup Language (AAPML – pronounced appmull) – a set of policy rules regarding the use of identity-related information from an identity source. AAPML allows identity sources to specify constraints on use of data provided by the source.
- CARML API – an API that makes it easy for developers to write applications that consume and use identity-related data in a way that conforms to policy set around the use of such information.
- Identity Attribute Service – a policy-enforced service for accessing identity-related data from multiple identity sources.

Where can I review the specifications and learn more?

http://www.projectliberty.org/index.php/liberty/content/download/3432/22922/file/Liberty_Id_Governance_mrd-v1.0.pdf

Spotlight on FiXs

Connecting Industry to Government

The Federation for Identity and Cross-Credentialing Systems (FiXs) is a coalition of commercial companies, government contractors, and not-for-profit organizations whose mission is to establish and maintain a worldwide, interoperable identity and cross-credentialing network built on security, privacy, trust, standard operating rules, policies, and technical standards. The FiXs network verifies and authenticates the identity of personnel seeking to enter U.S. military installations and other government-controlled areas, as well as commercial sites tied to the network.

"Providing a trusted identity authentication network between DoD and its industry partners signifies a new era for federated identity strategies and clearly demonstrates the commitment of industry and government to build more secure global identity management systems for physical applications," said Michael Mestrovich, president of FiXs.

Founded in 2004 and based in Fairfax, Virginia, FiXs was formed to pilot a federated identity transaction model and was incorporated as a not-for-profit corporation. A long-standing affiliation with the DoD credentialing program has enabled participating government organizations and industry members to establish secure and interoperable identity verification and authentication for secure facility and system access.

FiXs provides a trusted mechanism for federated identity infrastructure within and between public and private sector organizations with accuracy and trust through the application of a Federated Trust Model.

The network capabilities can be accessed worldwide, in remote or fixed environments, wired or wirelessly, and in real-time. A key component to the network integrity is its strong credential authentication and revocation processes, as governed by the FiXs operating rules.

The FiXs network uses available identity credential technology in conjunction with biometric identification. FiXs can be used within and between public and private sector organizations and promotes a trusted mechanism for federated identity infrastructures. The FiXs identity credentialing network currently is the only network certified to interoperate with the Defense Cross-Credentialing Identification System (DCCIS) infrastructure, the credentialing network of the DoD.

Remote FiXs components communicating over unsecured or public networks must support SAML 2.0. The project's SSO feature also supports SAML.

For more information on the project's current status go to:

http://eap.projectliberty.org/BODHome/docs/Mar2006/March_2006_BOD_FIXs_Cert_Reqts_USCG__Briefing.pdf

FiXs Members include:

3Factor, LLC

ActivIdentity

American Logistics Association

ChoicePoint Government Services

Disaster Management Solutions Inc.

Data Systems Analysts, Inc.

EDS

Eid Passport

Exostar

Imadgen, LLC

Johnson Controls, Inc.

Little River Management Group, LLC

Lockheed Martin Corporation

Northrop Grumman

SAIC

SRA International, Inc.

SRP Consulting Group, LLC

Unlimited New Dimensions, LLC

Wave Systems Corporation

Wells Fargo

WidePoint Corporation

E-Government Resources

Resources from E-Government Workshop: Brussels, Belgium

Go to:

http://www.projectliberty.org/index.php/liberty/resource_center/presentations_webcasts

There are several excellent presentations on current e-government deployments including:

- CATCert eIDM real cases and Identity Trends in Catalonia… Presented by Ignacio Alamillo of Spain, Catalan Certification Agency
- Strategy for the Use of eID and Electronic Signatures in the Context of E-Government…Presented by Katarina de Brisis of Norway, Ministry of Government Administration and Reform

SAML on YouTube

GOOGLE and SAML
http://www.youtube.com/watch?v=zrdscCoz4Lk

ProtectNetworks uses SAML and OpenID
http://www.youtube.com/watch?v=bDqvRAB7gTE&mode=related&search=

NTT Commuications Master ID and SAML-based SSO
http://www.youtube.com/watch?v=GTsB0Yv-NkI&mode=related&search=

- Mon Service Public…Presented by Gaël Gourmelen of France Telecom
- eID Trends in French E-Government…Presented by Alexander Tisserant/Benoit Boute of France, Ministry of Finance DGME
- VETUMA Electronic identification and signature service for citizens…Presented by Mira Nivala of Finland, Ministry of Finance
- Identity Trends in E-Government: Business…Presented by Thomas Roessler of Austria, EGIZ, E-Government Innovationszentrum

Deployment Workshop: Citizen Portal Success Stories, Oslo, Norway

For detailed success stories, presentations, and use cases from Norway, Finland, Denmark & Netherlands utilizing Liberty Alliance technology go to:

http://www.projectliberty.org/liberty/resource_center/presentations_webcasts

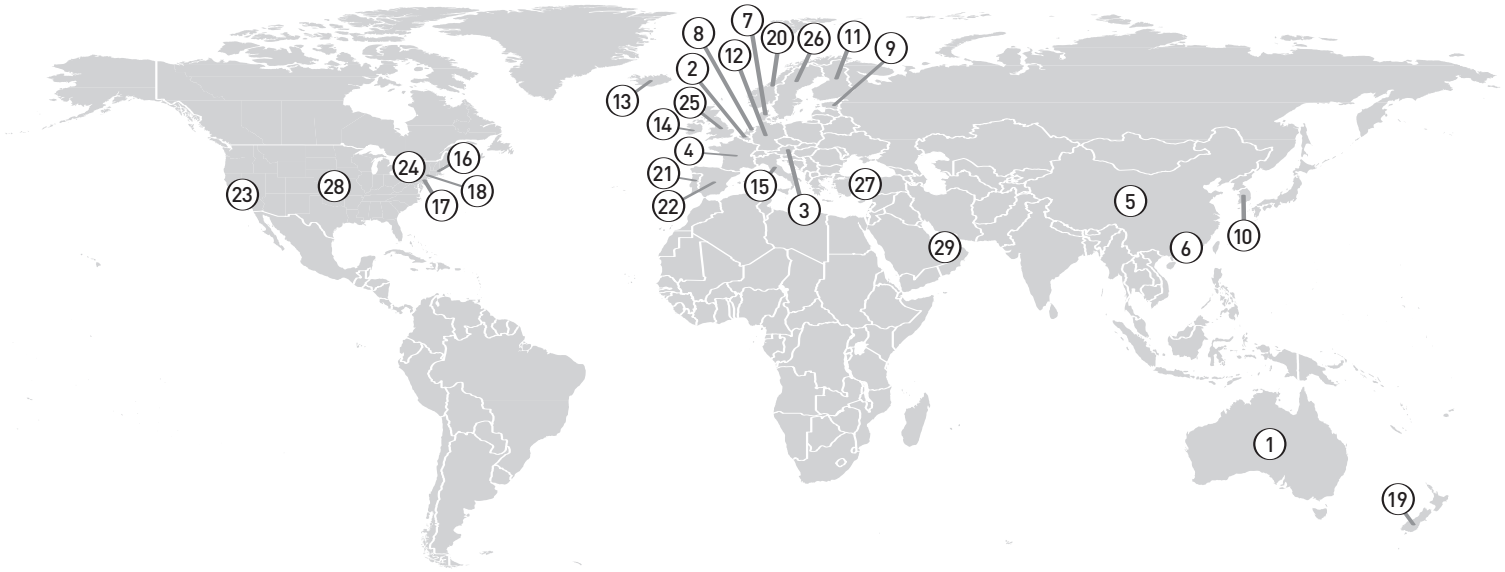
SAML 2.0 – Standard-of-choice in the Public Sector, 02/06/2007, RSA Conference

Presented by Conn Crawford, Sunderland City Council, UK; Georgia K. Marsh, E-Authentication Initiative, U.S.; Søren Peter Nielsen, Danish Government; Tero Pernu, Finnish Board of Taxes, Finland

Governments across the globe are adopting SAML 2.0 as the standard-of-choice in their federation solutions. This panel-based presentation is comprised of four case studies that provide an overview of current deployment scenarios and roadmaps governments have put in place for the wide-scale deployment of SAML 2.0. Open standards are helping governments meet regional regulatory demands and vendors worldwide are helping to facilitate the adoption of SAML 2.0 technologies. Go to:

http://www.projectliberty.org/liberty/resource_center/presentations_webcasts/saml_2_0_standard_of_choice_in_the_public_sector

Map of the World: E-Government Deployments



1. **Australia**—a Victorian state government project
2. **Belgium**—e-services for citizens and employers
3. **Austria**—Citizen Card enabling online banking
4. **France**—Public Service Portal; National Library, account authorization; Federated Identity for the French National Agency of Research; Cities of Pierrefitte and Vandoeuvre-les-Nancy
5. **China**—China Intellectual Property Net; National Development and Reform Commission
6. **SchenZhen City Special Economic Zone (China)**—Unified Identity Verification
7. **Denmark**—federated services in the public sector

8. **Netherlands**—Digital Identity for Citizens; A-Select Authentication System; Dutch Public Libraries
9. **Estonia**—Electronic ID Card
10. **Korea**—Integrated ID Management Services
11. **Finland**—Board of Taxes
12. **Germany**—Federal Government Employee Application; "Citizen Portal" electronic addresses
13. **Iceland**—Authentication Processes
14. **Ireland**—Reach agency, developing framework for electronic government
15. **Italy**—Ministry of Transportation Motorists' Portal
16. **Massachusetts**—e-services for citizens and agencies
17. **New Jersey**—Enterprise Identity and Access Management infrastructure
18. **New York**—federated multi-agency identity and access management
19. **New Zealand**—All-of-government Authentication Program
20. **Norway**—My Page portal for accessing personal information; Ministry of Government Administration and Reform; Norwegian Ministry of Education; Directorate of Public Roads; The Research Council of Norway; The National Library; Norwegian Ministry of Trade and Industry
21. **Portugal**—Citizen and agency e-government services
22. **Spain**—National Identity Card
23. **California**—Enterprise architecture and portal
24. **Pennsylvania**—Shared infrastructure services directed towards implementing a consumer-centric approach
25. **United Kingdom**—The UK Government Gateway Authentication Service; Sunderland City Council Smart Cards for travel and commerce
26. **Sweden**—Stockholm Portal
27. **Turkey**—Citizen and agency e-services
28. **United States**—Federal Government e-authentication and BIPAC
29. **Middle Eastern Country**—Security and passport control between people crossing the border between two Middle Eastern countries

Top Ten Reasons to Join the E-Government SIG

1 The SIG is focused on high-level collaboration and discussion among Liberty members with an interest in e-government identity management applications and services.

2 It's a one-of-its-kind forum to discuss best practices by government organizations on national, regional and municipal levels.

3 Participants can provide Liberty with subject matter expertise with respect to government-related requirements, use cases, challenges and future work items for solution in subsequent Liberty specification releases.

4 Participants get to take part in e-government–focused industry events.

5 It's a means to share solutions and/or technical approaches to avoid "reinventing the wheel" and to drive pan-jurisdictional adoption of standards-based identity management mechanisms in government.

6 SIG members can recommend liaison relationships for Liberty that will further the adoption and deployment of Liberty solutions.

7 It's where deployers and potential deployers can freely discuss the business and legal challenges associated with building Circles of Trust.

8 Participants get to contribute to deployment guidelines.

9 Liberty media relations looks to the SIG for spokespeople on e-government–related topics.

10 Participants can engage with the vendor community on a one-to-many "level playing field" that optimizes information sharing, efficiency and effectiveness without compromising government procurement rules.

For more information about how to get involved in Liberty's E-Government SIG contact: Colin Wallis, the SIG chairperson at Colin.Wallis@ssc.govt.nz

LIBERTY ALLIANCE

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**