

Case Study: **HP Drives Business Opportunities via Identity Management**

The Company

HP is a technology solutions provider to consumers, businesses and institutions, globally. The company's offerings span IT and telco infrastructure, global services, business and home computing, imaging and printing. HP has approximately 150,000 employees worldwide. Revenues for 2006 will exceed \$90 billion.

The Challenges

The HP IT organization is in the midst of a far-reaching, worldwide identity management (IdM) journey. To date, this effort has successfully focused on organizing and implementing a single identity management framework leveraged throughout the HP enterprise. The ultimate goals are to continually improve the customer, employee, partner and supplier experience; reduce provisioning costs; strengthen security throughout HP; and most importantly: drive new business opportunities.

Today, HP runs one of the largest customer identity management systems in the world. They have 21 million deployed users and are growing at a rate of 700K users a month. Getting to this point required a great deal of planning, focus, and willingness to just get out there and "do" federation.

“The main driver for joining Liberty at the time was that we didn't want to force our customers down a path of only centralized IdM systems. We wanted to offer an identity solution that was distributed. We wanted it to be open and, most importantly, we wanted the end-users to be in control. We felt it was very important to support Liberty and push for federation with a user-centric approach.”

Jason Rouault,
CTO of Identity and
Security Management
within HP's
OpenView group

HP Addresses Islands of Identity Management

HP began its IdM journey in 1999 as part of a security initiative. At this time, most of HP IT identity management was handled within several individual applications that then served various business units.

At that time, provisioning was being delivered via multiple, ad hoc, internally developed tools, and this was a growing problem. These tools were difficult to maintain and did not scale. Therefore, there was a need for automated provisioning. HP then decided to form the IdM Architecture Council to create one vision for IdM at HP IT, and decided to take a leveraged approach towards access management, provisioning, and federation. According to Anjali Anagol-Subbarao, Chief Architect, IdM, Marketing and Direct IT at HP, “We had different ID management systems we wanted to federate, and we also had many external partners. We saw that the opportunities were huge, but so were the challenges.”

HP Helps Launch the Liberty Alliance

HP joined the Liberty Alliance in 2001 as a founding board member, to help develop and deliver an open architecture and set of specifications to enable federated identity management. Their goal was to build upon the components of identity management by adding additional functions that allow for a federated model and puts the user in control of his/her own information.

At the core of Liberty specifications is the Identity Federation Framework (ID-FF), which facilitates identity federation and management through features such as identity/account linkage, single sign-on, and session management. These features represent the necessary encapsulation layer for work with heterogeneous platforms, security environments, and with all types of network devices, including personal computers, mobile phones, PDAs and other emerging products.

Definition of Terms

Identity (n) 1. the most basic element in a high value relationship 2. the individual characteristics by which a person, business, business partner, government agency or other entity is recognized or known

Single sign-on (n) 1. having the capability of accessing an online system once and having that authentication honored by other system entities, often service providers 2. sometimes called SSO

Identity Provider (IdP) (n) 1. a service that authenticates identity; often a trusted party such as a bank, mobile operator, or an

Internet Service Provider (ISP)
Service Provider (SP) (n) 1. a federation partner that provides services to an end user; service providers typically do not authenticate users but instead request authentication decisions from an identity provider

Federation (n) 1. an association comprising of any number of service providers or organizations 2. a model based upon trust in which user identities and security are individually managed and distributed by the service providers or member organizations 3. where the individual organization is responsible for vouching for the identity of its own users and the users are able to transparently interact with other trusted partners based on this first authentication 4. resembles the credit card model in that vendors accept an individual's ability to pay and then that ability is authenticated/verified through a single location

Circle of Trust (n) 1. a trusted group of identity and service providers who share linked identities and have pertinent agreements in place 2. where an individual or a business inputs a password once and minimal necessary credentials are shared among the Circle of Trust's members 3. a step strongly linked to federation, where multiple entities are involved, and there are business, policy and technical relationships in place 4. also known as “trust circle”

“The main driver for joining Liberty at the time was that we didn’t want to force our customers down a path of only centralized IdM systems. We wanted to offer an identity solution that was distributed. We wanted it to be open and, most importantly, we wanted the end-users to be in control,” explained Jason Rouault, CTO of Identity and Security Management within HP’s OpenView group. “We felt it was very important to support Liberty and push for federation with a user-centric approach.”

Rouault was instrumental in the early work on federation, serving as the chair of Liberty’s Technology Expert Group. “Jason led our Technology Expert Group through completion of the Federation Framework, the convergence of ID-FF into SAML 2.0, and the development of our Web Services Framework architecture and initial specifications,” said Brett McDowell, Director of The Liberty Alliance. “Few people possess the technical expertise, political acumen, and raw leadership ability that Jason exemplified during that critical period of our history.”

HP Becomes An Early Adopter Of Its Own Product: Walking The Walk

While HP IT was exploring ways to manage identity internally, HP’s software side was looking at how the organization could improve their identity management solution stack for HP corporate customers. “Identity is so strategic that simply partnering wasn’t a strong enough option,” said Rouault. “That led us to looking for key components that we could buy and build out as part of our overall enterprise sales strategy.”

In 2003, HP had already acquired Baltimore Select Access and TruLogica to fill out its solution needs in the identity and access management space. These acquisitions were then followed by the acquisition of the HP OEM partner Trustgenix for its federation technology. “The choice of Trustgenix was easy because of its broad coverage of the federation protocols, strong architecture foundation, and rich privacy-enhancing features,” said Rouault.

“ We had different ID management systems we wanted to federate, and we also had many external partners. We saw that the opportunities were huge, but so were the challenges. ”

Anjali Anagol-Subbarao,
Chief Architect, IDM,
Marketing and Direct
IT at HP

HP IT became a defacto customer of HP, and began implementing the OpenView solution. The benefits of having a large company become an early adopter of its own product are considerable. “We can obviously collaborate with HP IT and get, perhaps, more valuable feedback from them than we would from an external relationship,” said Rouault. “Even though we are both HP, HP IT really is another customer to us.”

This feedback was especially important during the early stages of the development process as both sides were trying to nail down requirements. “From the HP IT point of view, this back and forth was incredibly helpful,” said Anagol-Subbarao. “When we had an issue, there was always someone right there to work it through with us.”

Rouault described the relationship as “subtly synergistic.”

“From a product group standpoint, we had somebody we could work with closely early on to get real requirements feedback. From the customer’s standpoint—the HP IT standpoint—they had the ability to actually feed real requirements in that would meet their needs and solve their problems. It also gave them early access to the code—so it was very valuable for both sides. This has resulted in a very robust and scalable HP OpenView Identity Management offering that solves real business problems,” he added.

“ID-WSF is well-suited for business-to-business and business-to-consumer deployments where it is crucial to share attribute information in a privacy-oriented manner for online transactions.”

Jason Rouault,
CTO of Identity
and Security Management
within HP’s
OpenView group

Identity Management: Key Business Drivers

At HP, the objectives and drivers for wide scale identity management were formulated under the guidance of the IdM Architecture Council. They include:

Developing new business opportunities:

HP does e-business with a range of customers from Fortune 10 companies to small organizations. “We quickly realized that if we federate between them we can do a lot of cross-selling and increase revenue,” said Anagol-Subbarao.

Enabling the extended enterprise:

Companies like HP do a lot of outsourcing and partnering using identity management—especially federation. “The more we can promote seamless integration, the better for everyone,” said Anagol-Subbarao.

Reducing Costs:

At HP, costs were brought down or contained through a centralized identity management infrastructure.

According to Anagol-Subbarao, bringing up a complex Web site often costs upwards of \$2 million. If the site does its own authentication, it costs approximately four hundred thousand dollars. But if it integrates into a single-leveraged identity management framework, it will only be one-fourth the cost.

Mitigating Risk and Improving Security:

By using a single-leveraged IdM system, security roles can be more easily followed and rigorously enforced. Risk mitigation also improves. In addition, federation with customers and partners allows for secure seamless integration.

Enabling non-interactive principals (e.g., app to app):

This means that HP not only wants users to have access to ID management systems, but to devices, Web services and rich clients. This is all about looking at Identity Management as a business service and process, not simply as an application.

Moving Toward Loosely Coupled Web Services-based IdM Capabilities:

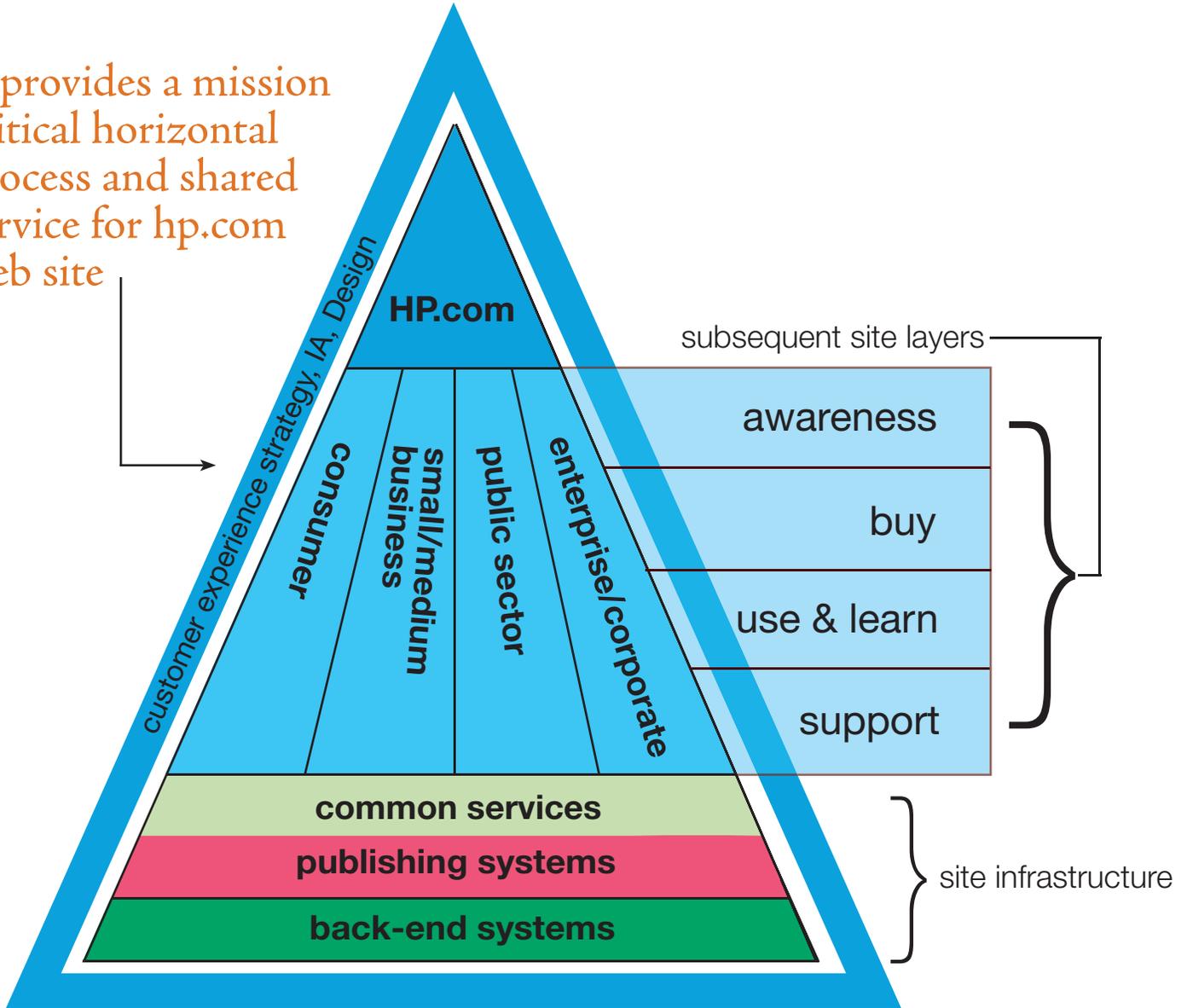
According to Anagol-Subbarao, Web services represent the future of identity management, and Liberty is a critical part of that future via the Liberty Alliance Identity Web Services Framework (ID-WSF). ID-WSF basically defines a rich and extensible framework for creating, discovering, and consuming identity services. This framework provides a Web services-based identity service infrastructure that enables users to manage the sharing of their personal information across identity and service providers. For example, a user will be able to authorize a service provider to access his or her shipping address while processing a transaction.

Today, HP is using Web services to do registration and authentication functions. "ID-WSF is well-suited for business-to-business and business-to-consumer deployments where it is crucial to share attribute information in a privacy-oriented manner for online transactions," said Rouault. "Relying parties in the transaction will be able to search and discover identity information from distributed identity services that the end user has registered. Policies related to attribute release can be defined ahead of time, or on the fly, via an interaction service that can communicate with the end user to obtain permissions."

“All of us who are deeply involved in federation know that you cannot sit lawyers down in a room and put together new contracts for every federated relationship. It’s simply not scalable.”

Jason Rouault,
CTO of Identity
and Security Management
within HP’s
OpenView group

It provides a mission critical horizontal process and shared service for hp.com web site



Driving the Business Case

Today, HP is building services to federate between these systems. On customer-facing issues, an ID management system is a mission critical service that manages access control registration services and user directories for all customer-facing activities. These Web sites are accessed through HP.com, and they include consumer, small business, public sector, and enterprise. These sites support all aspects of the customer relationship, from product registration and new product introduction, to customer support and selling HP products via Web storefronts. In addition to registration, authentication and authorization, HP.com also provides publishing via a centralized system.

When federating between these systems, security and privacy will be maintained via federation and implemented with the HP OpenView Select Federation solution. Controls can be specified by both the end user and the enterprise on what federation relationships can exist, what type of user information can be shared, and what type of consent is required. These privacy policies can all be specified down to the attribute level. As for security, it is inherent in the Liberty protocols and profiles of federation and attribute sharing.

“A great deal of time was spent by Liberty looking at the security and privacy considerations in various operating environments,” said Rouault. “This is what separates Liberty-based identity federation from other federation alternatives. Well, that and the fact that Liberty is truly interoperable.”

Today, this particular identity management system is one of the largest in the industry. As of September 2006 there are 21 million registered users and this number is increasing at a rate of 700K a month. It is also one of the highest available systems within HP and supports sites that do more than \$10 billion a year in business.

Anagol-Subbarao added that Liberty is ideal for deployment in the enterprise and business-to-business scenarios because of its SAML base. But Liberty is also ideal for business-to-employee and business-to-consumer scenarios. Its added facilities that make it privacy-friendly (for instance, pseudo-anonymity and anonymity) are a large factor for consideration—as are its support from multiple client types.

Lastly, because the Liberty Alliance has a conformance program to certify interoperability, consumers can rest assured that their vendor’s product has undergone the rigors of interoperability testing with other vendors.

More Work on Contracts, Agreements, and Trust is an Industry Imperative

When it comes to agreements and contracts, federation is like nothing that has come before it. Typically, in a federated environment, large sets of the user population are exposed to a business partner's application. In this scenario, risk and liability issues get magnified, especially when it involves sharing attribute information.

"All of us who are deeply involved in federation know that you cannot sit lawyers down in a room and put together new contracts for every federated relationship," said Rouault. "It's simply not scalable."

Rouault explained that these constraints have become well understood, because in federation everything is based on trust, and right now there are not dynamic ways to implement trust, and to define where there is liability and where there is risk. It's not as simple as earlier, more static relationships like EDI.

"The dynamic trust establishment is still quite a ways from becoming a reality," he said. "From a contractual perspective, we need to come up with a reusable framework about what companies need to think about when they put contracts together. I think this would help some companies at least convert some of their existing relationships and start reaping the benefits of federation with a limited set of partners."

Rouault added that this concern about how to deal with trust and liability is emerging as a stumbling block for federation newcomers—but that this is a space where Liberty has a focus and can have an enormous impact.

“Liberty has already made available the first level of ‘business guidelines’ for establishing trust relationships. There also has been some great work done for industry verticals such as Telco and Mobile,” he said. “Liberty is looking at providing the next level of detail, which will be focused on business and legal operating frameworks, and this will be enormously valuable to the industry. These frameworks can be thought of as a set of ‘templates’ for establishing trust agreements.”

What’s Next for HP

As federation and federated relationships expand and evolve, HP anticipates seeing identity federation becoming ubiquitous. Consumers, for example, should expect to see federation capabilities available in their phones, PCs, and other intelligent devices. These devices, working in conjunction with the user’s personal and privacy preferences, will be able to intelligently interact with service providers, applications, and other devices that may require identity information to provide a richer user experience or to conduct business.

From an enterprise perspective, Rouault said that HP agrees with its customers that identity management is a business service and process, and not simply a software application. This means that an identity management service should provide the core security, identity, privacy, federation, and audit infrastructure. Then it should be made available to the enterprise as Web services for reusable, modular and rapid integration with other enterprise applications. According to Rouault, this represents core and required technologies for Global 5000 customers.

HP is also addressing the convergence of network and user/application access control to have one integrated end-to-end access management system that is all tied to central uniform corporate security policies and virtualized identity stores. To that end, HP is investing to enable customers to securely

identify and manage every user, application, and device throughout and across organizations, and over time, to enable customers with flexible authentication, access control, and audit capabilities—while respecting privacy and regulatory controls.

On the product front, HP is integrating identity and access management with centralized systems, applications, and Web services management capabilities, as well as helpdesk systems, such as HP OpenView Service Desk, so customers can cope easily and cost-effectively with dynamic population changes. Rouault added that HP is also tracking and addressing the integration between change/configuration management and Identity Management systems. “Customers are readily integrating their software/application provisioning processes with their user provisioning processes to simplify operations, administration, and security management,” he explains. “This allows for a more responsive and dynamic IT organization that, for new employees, can provision both the user accounts and the relevant and authorized applications on their desktops/laptops/mobile devices. HP wants to be at the forefront of enabling this.”

ABOUT THE LIBERTY ALLIANCE

Liberty Alliance is a global alliance of companies, non-profit and government organizations developing open standards for federated network identity, interoperable strong authentication and Web services. Liberty Federation and Liberty Web Services provide consumers and organizations with a more convenient, privacy respecting and secure way to control online identity information. The Liberty Alliance management board currently consists of representatives from AOL, Ericsson, Fidelity Investments, France Telecom, General Motors, HP, IBM, Intel, Novell, NTT, Oracle, RSA Security and Sun Microsystems. Membership in Liberty Alliance is open to all commercial and non-commercial organizations. A full list of members, as well as information about how to become a member, is available at www.projectliberty.org/membership.