

Case Study:

Federation Gets Some (Political) Action

The Organization

Founded in 1963, the Business Industry Political Action Committee (BIPAC) is the nation's first business-oriented political action committee (PAC). BIPAC's mission is "Electing Business to Congress," and the organization provides expert policy analysis, research and communications on campaigns and elections, and fosters business participation in the political process. BIPAC also provides keen insight into which candidates for Congress are pro-business, committed to minimal government interference, and support free enterprise. BIPAC's members include half of the Fortune 100 companies and many small businesses, as well as pro-business national and state associations.

BIPAC has earned a reputation as the pre-eminent source of political intelligence for those engaged in American business. The organization is growing quickly and anticipates having 1000 member companies representing 50 million employees by the end of 2006.

"Having the correct agreements in place is so critical to achieving success in federated deployments. One of the strengths of the Liberty Alliance is their focus on business and policy guidelines. Liberty provided us with an excellent framework for how to handle authorization and authentication. Liberty Alliance is the only organization that offers policy as well as technology resources, and this makes all the difference."

Darrell Shull
VP for Political Operations
BIPAC

Challenges Around Tracking and Delivering Political Information

BIPAC tracks the positions of more than 59,000 elected officials, and provides voter registration information for the more than 3,000 counties around the country.

As a political action committee, BIPAC's challenge goes beyond the one-off proposition of simply providing information to a member corporation's senior executives. To really get the most out of the BIPAC relationship, that corporation must easily and securely deliver that information to all their employees. At the same time, they must be mindful of complex federal and state laws. Federal laws limit employer-to-employee political communications to clearly defined "advocacy" and "good government" messages.

This means that, for most employees, employers must restrict their activity to providing information on voter registration drives, incumbent voting records, candidate guides, grassroots involvement, and a wide range of other communications. An employer is permitted, though, to conduct PAC (Political Action Committee) solicitation and advocate for the election or defeat of candidates and parties—on behalf of managers, executives, and shareholders. This tiered provisioning isn't the only challenge employer's face. They must also deal with widely varying state laws where penalties for noncompliance include substantial civil fines and possible criminal charges.

“BIPAC helped deliver 40 million non-advocacy messages to employees in 2004, but up until recently, there really hasn’t been a good option for employers to provide PAC and advocacy information via the Web,” said BIPAC’s Darrell Shull. “We were looking for a solution that protected employee privacy, eliminated the need to give employee data to third-party vendors, and we wanted to provide relevant information without having the employee go through additional sign-on steps or registration.”

In the past, many BIPAC members who wanted to provide their employees with PAC and advocacy information relied on brochures and whitepapers. This was cumbersome and expensive. Others developed in-house communications tools, or contracted with third-party providers for authentication and content.

The problems with third-party relationships were significant. In order to enable authentication, employers had to provide confidential information about their employees to this outside provider. Whether the data is shipped manually or sent over the Internet, there’s a huge risk associated with both sharing and storing confidential employee information at a third-party site. Transfers of this data occurred on a monthly or other regularly scheduled basis, creating a significant lag time in provisioning or de-provisioning new or departing employees. And the costs were often significant — both in staff time and dollars.

In addition, BIPAC knew that employees didn’t want to go through all sorts of annoying steps to get at political information. They just wanted to click and get access. In fact, a recent BIPAC survey asked 1,000 voters the question: “If you were required to enter personal information to or register with a Web site prior to viewing, would you continue at that site?” More than 90 percent said they were less or somewhat less likely to use the site.

Moving to a Federated Solution with Sun Microsystems

For service providers like BIPAC, finding a way to streamline secure-information sharing was critical to growing their membership. Improved information technology and delivery was a critical element to their plans for the future.

Enter the concept of federated identity management: where users would have the ability to log in at one service provider’s site, and then go to an affiliated site without having to re-authenticate or reestablish his or her identity. To move to a federated model, BIPAC turned to Sun Microsystems and the Liberty Alliance, a consortium representing more than 160 global organizations. Liberty is the driving force behind the adoption of federated identity and has developed standards-based federated identity specifications to make easy and secure information access a reality. Sun was a founding member of the Liberty Alliance.

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”

In 2003, Sun was using BIPAC as an Application Service Provider, cataloging and providing good-government information to all Sun employees. Because there are no election law requirements for authentication when providing non-advocacy messages, access and site security were easy to manage.

So that Sun could expand its communications to include online PAC information, Sun and BIPAC then decided to partner to establish a new technology foundation leveraging the Liberty standards and Sun's identity management software solution. The plan was to test the model with Sun and then beginning rolling it out to other BIPAC members companies.

Addressing Secure Authentication and Authorization

One of the challenges BIPAC faced in this deployment was addressing the issue of tiered access. For example, if an employee desires to access additional, more restricted PAC content, there is a fair amount of personally identifiable information (PII) such as citizenship, level of employment, and/or shareholder status which needs to be collected and evaluated to determine the employee's eligibility. This information is required to authorize access to employer-provided PAC and/or advocacy content via BIPAC's Web systems. BIPAC and Sun needed to find a way to individually authenticate users who wanted to see restricted content while protecting personally identifiable information.

Second, BIPAC needed to deal with managing risk around authorization. Sun had the option of sending a batch of confidential employee information to BIPAC, but BIPAC didn't want to maintain a database of personally identifiable information. Sun also had the option of outsourcing the information to a third party which would in turn validate Sun employees and determine their level of access. Here again, such practices put confidential information at risk.

The Federated Model Eliminates the Need to Maintain Personally Identifiable Information

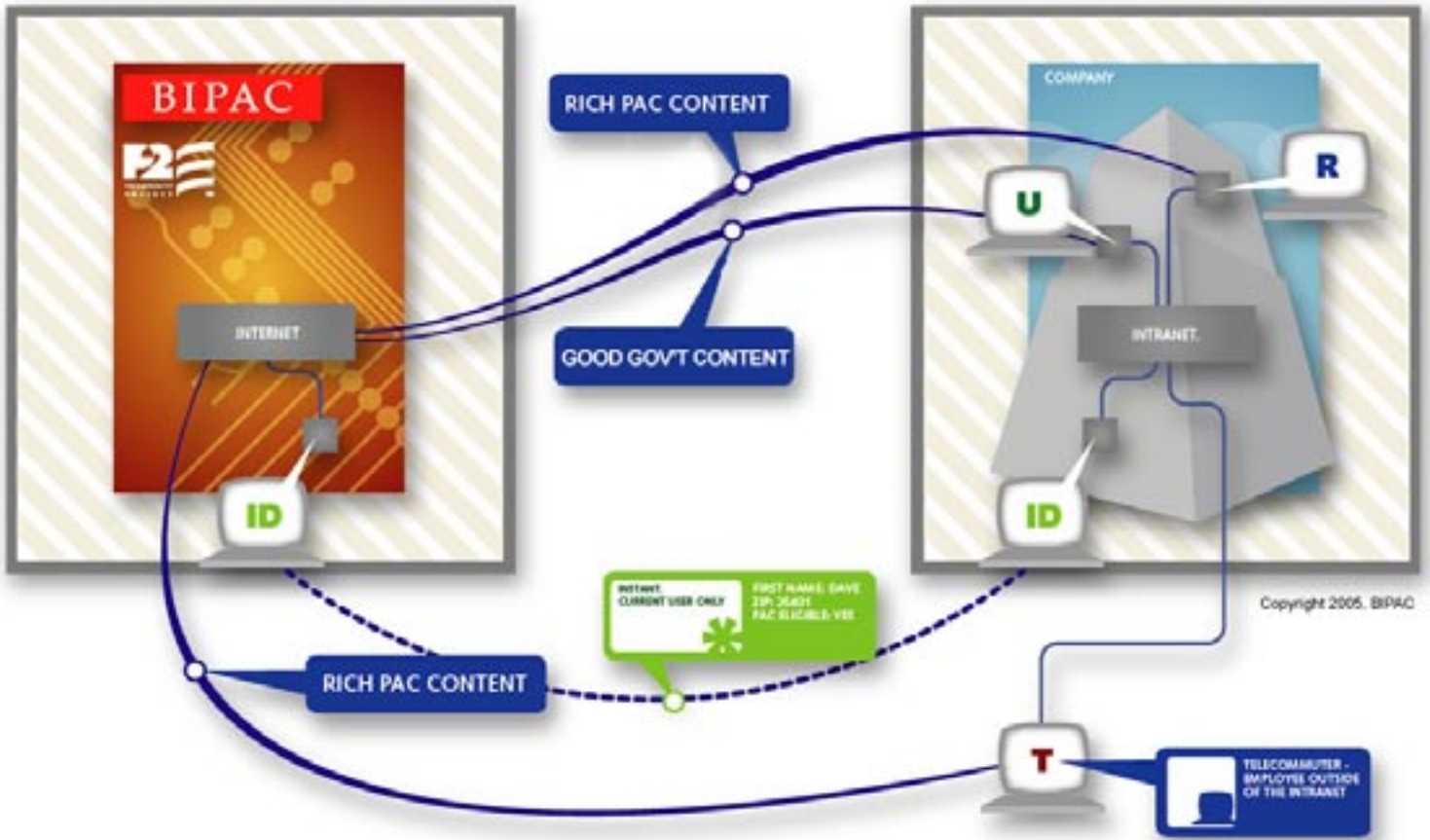
With BIPAC, single sign-on and federated identity have now solved the problem of securing personally identifiable information. Today, BIPAC member companies can manage their own resources, including employee and customer data. The solution enables BIPAC to delegate authentication of the user to the customer and does not require BIPAC to maintain this sensitive information. Federated identity management enables BIPAC to allow employees to be politically active without having to divulge private information — such as, social security numbers, home addresses, or phone numbers to third-party vendors — reducing the risk of identity theft.

There's an unexpected benefit here as well. BIPAC wanted to offer a service to customers that solicited PAC contributions from the customer's employees. This seemed unattainable due to FEC regulations and privacy requirements. Today, with the federated model, users can be authenticated individually without providing PII. Knowing their personal information is shielded and private gives employees the confidence to be supportive of an online PAC.

Added Security with Opaque Identifiers

Currently, many enterprises use an identity framework that involves a government-issued common identifier. These identifiers are static and portable, and therefore can easily be used at multiple Web sites if they are stolen. The Liberty model approaches the concept of identifying individuals differently by deploying an opaque identifier, which improves security and builds in protection against fraud/identity. Within the federated model, the Identity Provider (IdP) and the Service Provider (SP) together establish the opaque identifier, or a pseudonym to be used to refer to a Principal (user). Then all single sign-on communications use this agreed upon pseudonym.

The opaque identifier is valid only within the Circle of Trust and even if it were breached, the partnering companies could create a new one with no negative impact to the Principal. The opaque identifier is useless outside of that single transaction, and it's useless outside of the communication of that specific IdP and SP.



How the BIPAC Solution Works

Following Liberty Alliance Best Practices, Rules, and Guidelines

When it comes to setting up the federated model, it's not the technology which is difficult, but understanding the rules, guidelines, legal issues, and other key elements around business relationships.

"Having the correct agreements in place is so critical," said BIPAC's Shull. "One of the strengths of the Liberty Alliance is their focus on business and policy guidelines. They provided us with an excellent framework for how to handle authorization and authentication. Liberty Alliance is the only organization that provides policy, as well as technology resources, and this makes all the difference."

A Focus on Privacy

The Liberty specifications also emphasize privacy. A federated network identity delivers the benefit of simplified sign-on to users by allowing users to "link" elements of their identity between accounts without centrally storing all of their personal information. This increases security and delivers better identity control. With a federated network identity approach, users authenticate once in a trusted environment while still retaining complete control over their personal information. Liberty's open identity specifications have been developed based upon the principle that consumers should 1) have choice in what personal information they share, and 2) be able to give permission before data is passed on to others.

Enterprises which adopt the Liberty Alliance specifications for identity federation interchange are adopting standards which have a high level of security and privacy protection built in. As a result, identity interactions which operate under the Liberty Alliance specifications are also adopting standards which reduce the risk of fraud or security breaches through sniffing, hacking, replay, and other common online attack modes. In addition, federation limits the number of IdPs vulnerable to breach.

The Solution in Action

Acting as the identity provider, Sun is responsible for maintaining and managing the identity information of its employees, and providing them with a simple way of being authenticated. When a Sun employee first navigates to the BIPAC site, he or she is redirected back to the Sun Java System Access Manager™ for deployment. Typically, the employee would have already accessed some of the internal systems and therefore already have an existing login session. This system would, in effect, already recognize the user and then redirect them to the BIPAC site without showing a login prompt. Only if the user didn't have an existing login session would he or she need to be authenticated.

The Sun Java System Access Manager helps BIPAC manager secure access to its Web applications both within the organization and across business-to-business value chains.

The Access Manager meets the current needs of the enterprise for secure protection of essential identity and application information. It also supports BIPAC's future business needs and tighter integration with business partners through the implementation of the latest Liberty standards. Sun's Access Manager is also the first commercially available product to support Liberty Alliance Phase 2 Identity Web Services (ID-WSF) and SAML 1.1 and SAML 2.0. The Sun Java System Directory Server™, another key part of the solution, offers a solid foundation for BIPAC's identity management needs by providing a central repository for managing identity profiles, access privileges, and updated attributes.

Extending the Model to the BIPAC Membership

With such a powerful solution, BIPAC has the opportunity to create deeper relationships with member companies, providing a wider range of political information services and PAC tools, such as online contribution systems, which automatically and seamlessly integrate with federal and state reporting systems. Employers who spent substantial time and money working with third-party vendors to provide authentication and authorization services can now dedicate those resources to more productive communications with employees about candidates, issues, and elections. And the ease of implementation and security of the Liberty solution makes it easier for BIPAC to convince more companies to start providing good-government and PAC information to their employees.

Today, the organization is extending Liberty and federation to other member companies. Darrell Shull estimates that by the end of 2006, ten organizations representing more than 500,000 employees will be up and running on the system. Liberty and federation has served as a market differentiator for BIPAC, setting it apart from the third-party vendors who have not always treated private employee information with the care it deserves.

BENEFITS OF FEDERATION TO BIPAC MEMBERS

- Improved experience through single sign-on
- More control over personal information
- Faster access to political information and resources
- Better risk management policies
- Easier and more secure provisioning of resources
- Better control of PII

BENEFITS OF FEDERATION TO BIPAC

- Improved service offerings
- More integrated relationships with members, suppliers and other partners
- Better security
- Faster information delivery
- A means to replicate the federated model and provide it to others

TECHNOLOGY DEPLOYED

- Sun Java Access System Manager
- Sun Java System Directory Server Enterprise Edition

About the Liberty Alliance

The Liberty Alliance Project (www.projectliberty.org) is a global alliance of companies, nonprofit and government organizations developing open standards and business, policy, and privacy guidelines for federated network identity. Federated identity offers businesses, governments, employees and consumers a more convenient and secure way to control identity information, and is a key component in driving the use of e-commerce, personalized data services and identity-based Web services. Liberty specifications are deployed worldwide by organizations that include American Express, AOL, BIPAC, General Motors, Fidelity Investments, France Telecom, Nokia, NTT, and Sun Microsystems. Membership is open to all commercial and noncommercial organizations. A full list of Liberty Alliance members, as well as information about how to become a member, is available at www.projectliberty.org.