The challenge of federated identity management

Don Smith, technical director, dns

In an age where identity management is becoming an increasingly important issue for both businesses and individuals, the concept of federating it is attractive. Federated identity management allows for an economically efficient and convenient way of delivering identity services between different organisations.

Don Smith

Identity management 101

Centralised identity management models were first created to help deal with user and data security on the same network. Then, business models began embracing new concepts such as enterprise virtualisation and outsourcing. Unsurprisingly organisations seeking to implement these models sought to leverage the internet as a transport, and web-enabled applications as a delivery mechanism.

In this new world, users must be able to easily and securely access data and services in organisations other than their own. Federation technologies first appeared with the aim of offering web-based single sign-on across organisational domains.

A basic example of a federated system in action could be that of a university, in which students use a single identity and achieve single sign-on to access library books and journals from both their own library and that of other academic institutions. The university in which the student is enrolled is responsible for maintaining their identity and authentication credentials. Other institutions would rely upon this information when authenticating the student.

Aside from the obvious convenience to organisations and their end-users, there are equally clear security advantages. Managing the lifecycle of user identities and accounts can be a challenge, particularly when someone leaves an organisation. When spanning organisational boundaries it is almost impossible to do so without strong processes. Federated identity systems can help.

Multiple corporations can in theory, share a single application, which results in cost savings and consolidation of resources. Such technologies are aimed not just at commercial enterprises, but at decentralised organisations like the military and the government, who are able to use such applications as a means of linking business units and internal departments.

So, on a basic level, federation does seem to be a realistic and effective method of enabling cross organisation authentication. In 2005 there were predictions of a rapid acceleration in the adoption of federation, but, across the board, this has not been the case and it is only by looking further into the technology, how it works and how it is used that we can identify the reasons why.

Federation standards and technologies

Federation standards have been in development for several years now. They are relatively mature and well understood. Federation standards are supported by a number of bodies such as WS-*, Oasis, and the Liberty Alliance. Each body supports different standards, which can be inter-related. However support for the standards is widespread. Software vendors such as Novell, Oracle, Ping Identity and Sun have invested in federation and have established products which support the various standards.

The security assertion markup language (SAML) is an excellent example of a federation standard, having been approved by the Organisation for the Advancement of Structured Information Standards (OASIS) in 2005 and backed by the Liberty Alliance's interoperability testing in the same year. In August 2005 vendors such as Sun, Oracle and Novell were amongst eight who secured the Liberty Alliance's seal of approval on SAML 2.0 interoperability testing.

How federation works

Federation technologies provide open, standardised and secure methods for a service provider to identify users who are authenticated by an identity provider. The technologists would rephrase this as a relying party (RP) which is consuming identity assertions supplied by an asserting party (AP).

In our university example, the home university is the AP and the remote libraries are the RPs. The user identifies themselves to their home university and then connects to an external library service and authenticates (transparently).

The real challenges facing identity federation

Three years ago the technology was ready, there were approved standards in place and major software vendors were ready to implement. It is therefore unsurprising that experts were predicting

rapid growth. This growth has not happened. What's going wrong?

In many ways the technology obfuscates the problem. While identity federation is not rocket science, there's confusion about what it delivers and the complexity involved. Whilst mainstream in terms of vendor support and standards, the language used to describe federation concepts is cumbersome and inaccessible. This all leads to a focus on the technologies, which is counter-productive.

"The experts were predicting rapid growth. This growth has not happened. What's going wrong?"

The fundamental concept underlying federation is trust. The RP must trust the AP to both manage their users and to authenticate those users on behalf of the IP. However, trust is difficult to gain and easy to lose. Furthermore, while there might be a willingness amongst individuals to establish trust relationships with third parties, this might not be achievable at an organisational level. The benefits of federation are felt by larger organisations, where agility in establishing trust is not natural for most.

People and process

Identity management is about people and process. Organisations are challenged enough by internal identity management issues without extending this to external partners or service providers. Identity management projects require momentum from more than technologists. They are business projects and require sponsorship, leadership and cross-functional buy-in.

Federated identity management is not an infrastructure project. Even with a willingness to proceed, implementing cross-domain single sign-on might not be easily achievable. The fortunate will find that implementation is straightforward and integration with their existing application park is easy. The unfortunate might find that they need to identify or drive an application refresh, which can be used to introduce web access management technologies in support of federation.

Liability may also be an issue. In the wake of current data leaks, companies must check on the potential liability of the federated partners who might fail to follow proper process relating to the identification of their employees. False identity information and weak password protection can lead to potential data loss and security breaches.

Many companies might be struggling with the complexity of the options available, and may be in the dark about the best route to take. These are skills which may exist in-house, but this is true on rare occasions. Often, a safe and cost-effective route is to work with experts in the field, to clarify your identity management drivers, quantify your return on investment figures and ultimately deliver a project with real business benefit.

Federation in action

Adoption of federation is in some cases already well established within 'communities of trust'. Examples of this include higher education environments. Eduserv Athens is used extensively across UK higher and further education institutions.[1] With the Classic Athens service, Eduserv acts as the AP authenticating users on behalf of many service providers (typically libraries). Athens Local Authentication allows individual institutions to act as their own AP.

Boeing has also successfully implemented a federated identity deployment. Like most large corporations, it manages a large benefits program that serves both current and past employees. The various accounts (from retirement benefits to medical) associated with these groups were managed by 24-hour hotlines for individual accounts. By implementing federated identity management, the company could collapse all of those desks into one while improving satisfaction and reducing costs.

This system allows Boeing's employees to access more than 1000 protected websites and resources through single sign-on, with an internal portal that is used every day by employees including a connection to various external benefit providers. This eliminates the need for multiple passwords and connections to assorted institutions.

Service providers are also starting to realise the benefits of federation in lowering costs by devolving user management back to their customers. Google Apps isn't the only service supporting SAML authentication. Postini, the search giant's recent email security acquisition, also supports SAML for user authentication to its quarantine areas. This is a likely growth area for federation. Even though service provider margins are thin, the emergence of open source federation implementations such as OpenSSO make the implementation of templated federation deployments a low cost option.[2]

User centric identity management – identity 2.0?

No commentary on federation today would be complete without a sideways glance at the world of user-centric identity management. In the business-to-consumer world, the industry is now seeing the emergence of user centric identity management. This gives promise in delivering users greater power and strength over their own profile and user experience.

"Can you take your eBay feedback rating anywhere else? Can you recover your social network from Facebook?"

Today we all have multiple independent identities in existence on the internet. Consumers interact with sites like Amazon, eBay and Facebook, but there is no electronic link between these different identities (except, unfortunately, often a common password). It is an annoyance to consumers to maintain their identity information securely on multiple sites.

Increasingly it's also the case that consumers are realising that they don't own their own identity on these sites, or at least not the items of value. Their existence on the internet is siloed. Can you take your eBay feedback rating anywhere else? Can you recover your social network from Facebook?

The response to this consumer pain is twofold: Microsoft Cardspace and the OpenID initiative. The aims of the two schemes are similar, and Microsoft has announced that its system will interoperate with OpenID.

Cardspace allows consumers to store attributes of identity information storing them in one or more InfoCards that can be presented to Cardspace-enabled applications or websites. The user controls who can see what attributes of identity information, and manages it on their local client.

Inside OpenID

OpenID is similar in aim, but different in implementation. Instead of storing an identity locally, the user chooses an AP on the internet. The AP is then referenced providing a URL to OpenID-enabled sites during authentication.

OpenID is similar to federation in that there is separation between AP and RP, but it is crucially different in two ways. Firstly, it is decentralised. The AP could be any OpenID-enabled AP. Secondly, the process that establishes the trust relationship differs. In traditional federated identity systems, the RP establishes a trust relationship with a set of APs of its own choosing. In the OpenID model, the RP will trust an AP only for the users that assert it to be trusted, and only when told to do so by the user. The fact that this trust relationship doesn't have to be set up in advance is a requirement for consumer deployment, but is also key advantage of the OpenID technology.

Support for OpenID

In January 2008, Yahoo! announced it would become an OpenID Identity Provider for all of its existing user accounts, and by February had added 280 million consumer accounts to those that could be used within an OpenID framework. In February it was also announced that Google, IBM, Microsoft, VeriSign and Yahoo! had joined as its first corporate board members. OpenID certainly has gained some significant momentum and credibility in recent months.

A cynic might point out that there's a lot of momentum in becoming an OpenID AP rather than an RP and this is true. OpenID's decentralisation is designed to give independence to identity ownership, but cynics might observe that organisations are using it to capture identity, as owning identity seems to add value to organisations these days.

There are still usability concerns around OpenID. Remembering your OpenID identifier could be one challenge, but it's certainly interesting technology which shows real promise.

The future of federated identity management

It is clear that there is not likely to be a overnight revolution that will bring federated identity management into our everyday lives. It is more likely to be an evolution and some might argue that this is already happening as it enters communities of trust such as higher education.

We have also seen the example of OpenID where consumers are able to manage their own identities, and it is these areas, perhaps more than in the enterprise, where we will see rapid adoption of federation-like technologies.

The current wave of internal identity management projects in enterprises may be laying the foundations for federation in the future. As more organisations solve their internal user management problems, they will look to employ their technology investment to manage their external users.

Trust and organisational agility continue to be the stumbling blocks for adoption of mainstream federation technologies. Identity management is about people and process, rather than technology. In summary, federation needs help. The technology needs to be emphasised less, the concepts need to be emphasised more, and the delivery must be seen as more strategic to organisations. All of this will help establish the momentum that it needs to succeed.

References

1. Athens overview page, Eduserv <www.athensams.net>
2. OpenSSO project page, OpenSSO project <https://opensso.dev.java.net/>

About the author

Don Smith has worked in the IT industry for 17 years, and began his IT career with the groundbreaking Edinburgh University spin-off, Vision Group. After Vision was acquired by STMicroelectronics, Don became responsible for security architecture and operations in Geneva for this $8billion enterprise. Don joined dns on returning to Scotland in 2005, and since joining has been instrumental in the ongoing development of the dnsMSS service portfolio.