

The Evolution of Federated Identity Deployments

BY LINDA ELLIOTT



As real world federated identity deployments occur, a pattern is emerging for how they begin and evolve. Each company that approaches federation is likely to travel a path similar to those that went before, and issues of technology, standards and business impact are more easily understood if they are viewed as part of this bigger picture.

Federation is becoming real. Some federations are becoming well known through descriptions in published articles and conference presentations, and there are many newer and smaller federations emerging in various market segments. We are beginning to see a pattern of deployment that reflects the practical business requirements of the environment as well as the state of maturity of the technology, and we can start to draw conclusions from this pattern.

The Pioneers

Many of the more noted federations were established before the current versions of federation technology specifications were available. As a result many of them use variations and customizations of what was available at the time they were first implemented. The willingness to make those essentially custom changes in order to get a working federation underway provides an indication of the motivation and focus of those early movers. The industry should thank these pioneers, for without such efforts we would not have some of the refinements present in newer versions of the federated identity specifications and we might not yet have the awareness of how important federation will be.

Today, federations are emerging in many industries and for many use cases. In most cases, they are now able to use federated identity technologies as specified.

The use cases now deploying most often revolve around employees gaining access to outsourced services, collaborating with employees at partner companies, and engaging in supply chain activities. These are more controlled environments than those which involve consumers and individual customers, and hence they are comfortable places for many corporations to begin.

Early Experiments

Many companies begin their forays into federation with the most controllable situation possible – an internal federation between various security domains. This generally does not include all domains within a corporation, but is really a tentative and experimental step involving only a few domains. Without external visibility, these experiments are easy to watch and control, and any downside can be contained internally. Fortunately, these experiments can lead to the realization that it is not really necessary to combine all of the various enterprise domains that may have sprung up from M&A activity or independent divisions. Happily, federation can turn out to be an easy way to integrate domains without moving to a single consolidated Enterprise Identity Management system which can be both costly and time consuming to implement. If an enterprise already has a unified EIM, however, then this step may not be on their migration path.

The most-often observed first step in external or cross-domain federation is a

The hub company has decided to expand its federation in order to provide more value or save on administrative costs.

federation between two partner organizations who already have a contract with each other. The partners typically have an existing process which uses either private electronic connections or internet connectivity. The partners agree that federation will reduce the friction of connectivity and also vastly reduce the overhead of maintaining their respective provisioning processes.

Typically, technology decisions in these deployments are driven by one company, the one who sees larger federations as key to its business strategy or to enhancing its position in the market.

services to many companies). The critical issue is that the hub company has decided to expand its federation in order to provide more value or save on administrative costs.

During the time that the hub company is expanding its federation, it usually begins to consider the issues of managing a federation relationship with multiple partners concurrently. In addition to any existing contractual relationships, this is when specifics related to the federation get aired and the complexities of multiple concurrent relationships come to light. Key issues raised by business

These more sophisticated capabilities are only beginning to gain attention in standards bodies.

Since usually these partners are already working together in some electronic mode, they generally don't address any liability or trust issues in that contract, or in a new contract. Rather they rely on the legal structure they already have in place and assume that will cover any issues which may arise.

Expanding Federation

Once a company has tested its federation strategy with a single trusted partner, and found that the technologies are effective, it can consider building a federation of multiple partners. In this case the company is considering becoming a hub, and in fact this may have been the goal when they first tried a federation with a single trusted partner. The hub might be the identity provider (a company whose employees need access to several outsourced services) or the hub might be a service provider (an ASP for

managers and legal counsel include the risk and liability of the federation model, handling user privacy issues, complying with regulation such as Gramm-Leach-Bliley or HIPPA, dispute handling, and consistency across all relationships. Most federations at this stage settle on a standard bi-lateral agreement which they intend to use with each partner.

Success and Complexity

As hubs continue to add more participants to their federations, a truly frictionless approach to web-based business becomes apparent. A few issues will begin to crop up. Some of these are associated with the state of the industry for federation-enabling products, others are simply the result of success. Today, specifications continue to mature, and new versions of all widely-adopted specifications are being released regularly. One issue that arises is whether to upgrade

The industry is moving fast, and by the time that most federations decide to take the next step products will be appearing with these features in them.

all partners, operate on several versions concurrently, or stay on the initial implementation. This decision will be based on the need for newly released features of federation products and the specification versions they are built on. As the federations themselves mature, the partners may decide that its time to implement features such as dynamic provisioning and de-provisioning of accounts, or posting and enforcement of access or privacy policy. These more sophisticated capabilities are only just now beginning to gain attention in standards bodies and are not available in most federation products. However, the industry is moving fast, and by the time that most

Visa, MasterCard, ACH, and SWIFT all are examples.

There are a few examples of such approaches for identity federation. Shibboleth, the anonymous federation approach adopted in many academic institutions for research and library access, came to this conclusion and is now launching a common set of operating regulations for its participants. The Electronic Authentication Partnership (EAP) is a public/private partnership which is attempting to create common rules specifically for the credentialing and authentication pieces of the federation model. PingID has created operat-

will appear, such as a health provider federation that unites specific instances that evolved in different places with various hub drivers. For this to happen, the market will need to produce more sophisticated tools such as automated policy and regulation compliance checking. Additionally, the need for common rules and processes will need to gain traction as federations include more and more enterprises. Market leaders are already aware of these needs and are already pursuing solutions.

Not all enterprises will follow the same path of evolution. However, by examining what is already apparent in the mar-

Federations with multiple partners will begin to face the complexities of pair-wise agreements in an ever expanding federation. Quickly the universe of bilateral agreements becomes unmanageable.

federations decide to take the next step in sophisticated federation management, products will be appearing with these features in them.

Governance and Agreements

On the business management side of the picture, federations with multiple partners will begin to face the complexities of pair-wise agreements in an ever expanding federation. Very few hubs will avoid the need to make a change here, another there, to accommodate key partners. Quickly the universe of bilateral agreements becomes unmanageable. At this point, large federations begin to consider the approach used in most large business networks – a common set of rules to govern the relationships and treat everyone with an equal footing. The financial networks have been most successful with this approach;

ing regulations for identity federations and offers its Network as a ready-made vehicle for adoption of these rules between the participants in a federation.

Linked Federations – the Future

The great question which has not been answered is whether federations will take the next step – to join their federations together, creating a unified environment where many hubs, many identity providers and many service providers exist under a unified structure. There are varying points of view about whether this is truly feasible as market verticals (health, financial, telecom) as well as business orientations (B2B, B2C, G2C) may have impediments to integration in their rules. However, few argue that market specific federations are feasible and probably

ket today, we can see that the needs of business and the innovation of technologists are moving us steadily towards a new mode of operation where federation makes the online experience much more like what we always hoped it would be. ■

Linda Elliott is VP of Business Solutions at Ping Identity Corporation. Prior to joining Ping, she spent 15 years as a senior executive of Visa International where she both built and managed Visa's global transaction network. Ms. Elliott's roles at VISA included EVP of Payment Systems, Strategy, and e-Commerce developing the first implementation of online authentication for card authorization using PKI technology, and managing clearing and settlement systems that handled \$3 billion in daily transactions in 26 currencies.