

# Federation – the Final Frontier?

BY ARCHIE REED



---

Federation is the hot Identity Management conversation and has been billed as the way to create a frictionless method for consumers and businesses to follow processes across any number of sites and administrative boundaries. Delivering federation, however, has so far been mostly thought of in security and technology terms, which makes it difficult to see what is really required to deliver its promise.

---

**F**ederated identity is ultimately about bringing borders down and making freer trade possible between organizations, their customers and value-chains. The market has used different terms over time to describe this process – EDI, B2B and most recently, Federation. At issue is finding methods that deal with the security implications of these changes while simultaneously capitalizing on the potential of closely integrating business processes.

In the IT and security space the technology challenge has been described as the disappearing perimeter. Translated into business terms, however, it is about creating the ability for business relationships to be easily established and managed between organizations. A combination of technology and process management is thus essential to succeed.

At the core of any business process is identity. Understanding who you are dealing with and understanding the context of the deal is critical to managing risk. Because there is a high possibility for businesses to be negatively impacted when something goes wrong (e.g. security and privacy breaches, financial losses), the federated identity discussion has focused heavily on security and technology. However, the real cost in identity management isn't in technology, it's in the process management. Meta Group estimates that 65% of the total cost of Identity Management is

related to integrating with business processes while Gartner estimates it as high as 80%.

It is therefore critical to determine how you will respond to changing conditions and process requirements. This is also why the ability to provide quick deployment is not the only parameter on which to judge the value, or ROI of identity management solutions to your organization. How a solution enables business processes changes, after deployment, is also a critical factor.

## The Evolution of Federation

Federation is actually a pattern that has existed for some time in most organizations. It is important to note that we have had a lot of legacy examples of federation which can provide significant learning opportunities. So far, we can see three distinct types of federation evolving, Internal-, Extended-, and Cross-Enterprise.

**Internal Federation** – Often, organizations already understand the basics of federation internally. Both IT and Lines of Business have developed and deployed solutions that required integration. This first generation of internal federation included directories, synchronization, and basic identity and access management tools. These tools provided a level of integration beyond simple data level integration, and allowed for internal process integration.

*continued on page 68*

continued from page 72

Lines of Business (LOB's) often deploy and manage their own applications. LOB's also demand the ability to manage their users and service offerings. As a result, organizations often find their business hierarchies look like fiefdoms with separate LOB's often having their own IT staff and budget, yet still requiring resources and services from centralized IT and security units. Central IT ultimately owns the accounts and shared resources, and must maintain "control" over identity and security. From this structure we learn that the politics and stakeholders of an organization have a significant impact on its ability to succeed. It follows that there must be a way to integrate the control of both identity and business process between these entities within the organization while allowing some form of process change throughout in a delegated administration framework.

This is similar to the classic problem of Government.

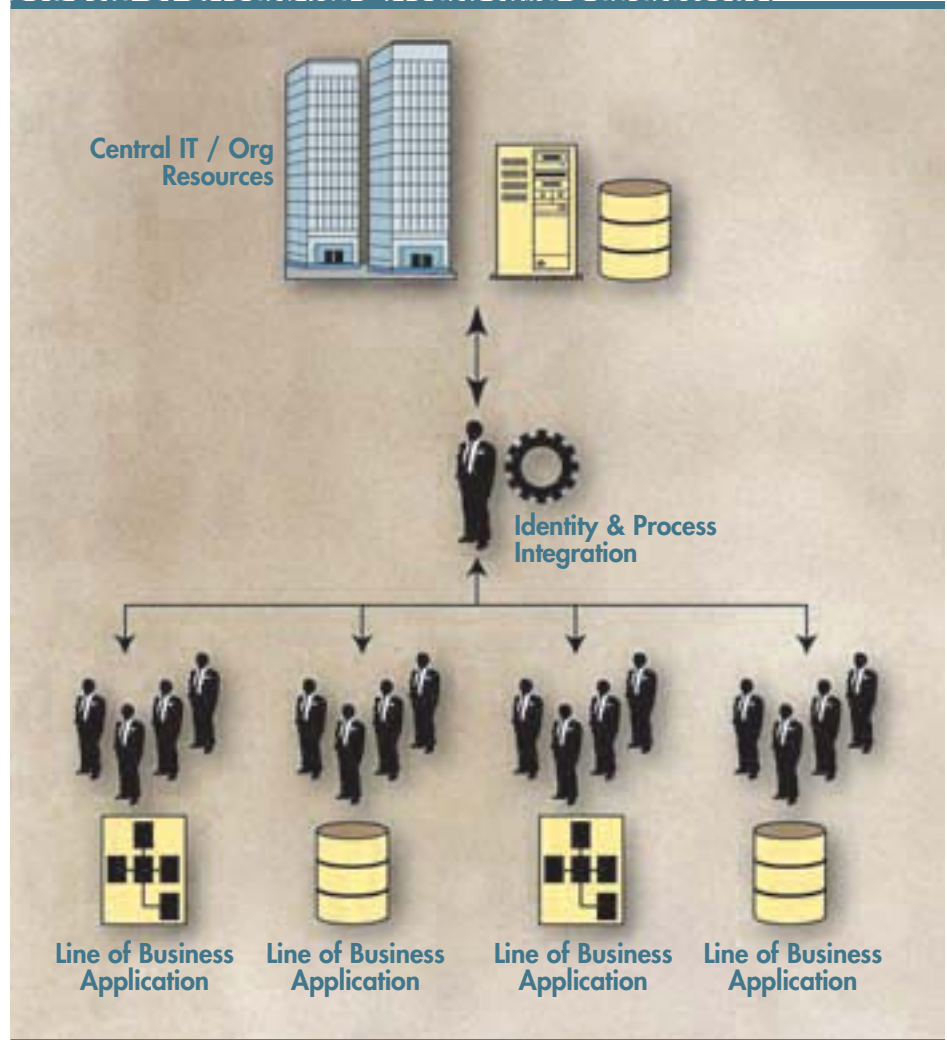
- **Central government**
- **Separate states, provinces, etc.**
- **Local requirements**

These model the evolution and general requirements of broader federation, requiring differing levels of trust, delegation, regulation, policing, contribution, and understanding.

**Extended Enterprise Federation** - In extended enterprise federation, we see a classic business model of one organization offering its services out to one or more organizations. This is a service provider model where all the capabilities or resources are controlled by the central party. This closely parallels the classic IT department offering services to lines of business seen with Internal-Enterprise Federation.

**Cross Enterprise Federation** - Cross enterprise federation occurs when any number

FIGURE 1: INTERNAL-ENTERPRISE FEDERATION



of organizations group together around business processes to enable each other to provide and consume services together.

The challenge with Cross-Enterprise Federation is that most standards efforts today are focused on security and access management. However, throwing authentication at a wall and hoping it goes through the window is not scalable or secure. There must exist an ability to delegate process and workflow controls across organizations. This means that workflows require the ability to be passed across organizations, be executed, signed and returned to the original process manager such that the result can be audited.

The concept of offering and securing services becomes clear when we look at this evolution. Thankfully the direction most initiatives are taking involves a serv-

ices based approach to begin with. However, the capabilities used to create these links are simple lookup and use technology. We need to consider the additional implications inherent in any cross-enterprise offering.

Examining internal federation experience shows that the critical functionality required for successful internal federation is 1) Delegation and 2) Self Service. The level to which these are available, however, varies significantly based on the level of trust between organizations, and the level of trust in the supporting infrastructure and processes. Cross-Enterprise federation adds to that the very real needs for contractual agreements, mediation and legal remedies.

Examining the current levels and capabilities of Internal Federation makes it clear

that there are many technology challenges remaining in the Extended and Cross Enterprise Federation models. However, business and legal processes are even more critical building blocks than technology.

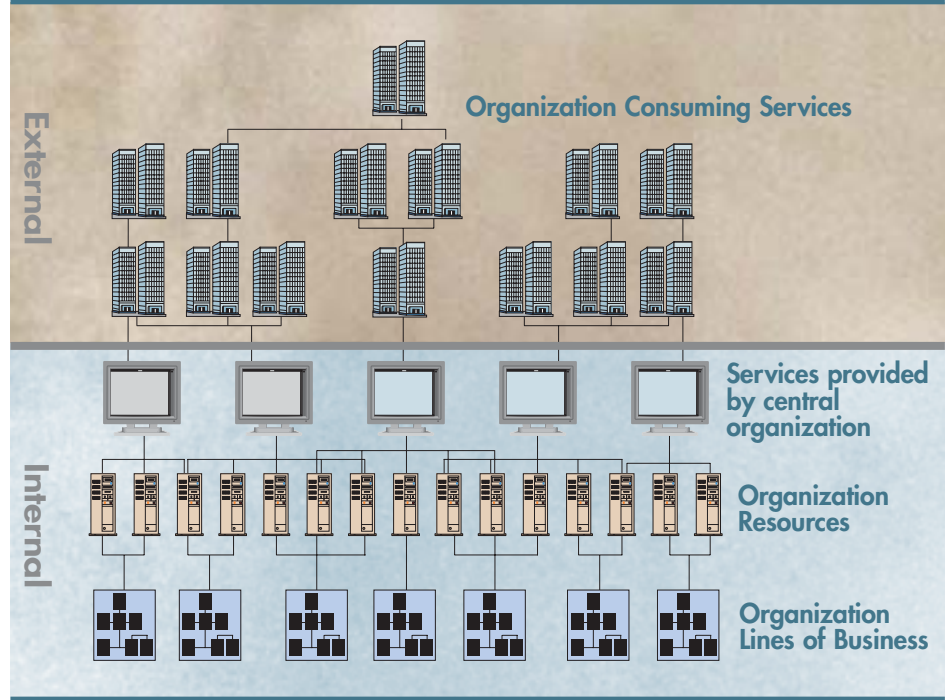
### Security is Important, but Business Process is Critical

The cost of breaching security is coming down, while the cost of protection is rising. The only way to manage this challenge is through careful process controls. This means that removing the friction to changing processes is an essential requirement of extended- or cross-enterprise federation technology.

As the barriers and perimeters come down in cross-enterprise efforts, the market has seen a number of high profile efforts to address the potential federation requirements in terms of identity. Starting simple, as many successful standards efforts have done, we find the OASIS Security Assertion Markup Language (SAML), the Liberty Alliance and WS-Federation.

By taking a purely technology or security based approach to federation, however, we only create partial solutions. Today's Role

**FIGURE 2: EXTENDED-ENTERPRISE FEDERATION**

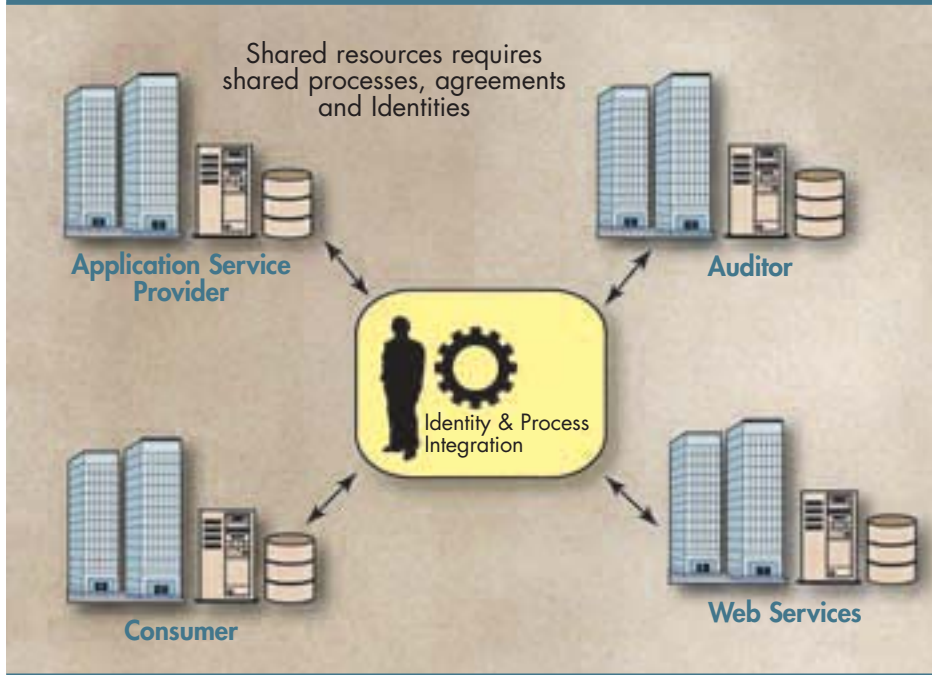


Based Access Control (RBAC) solutions do not tightly integrate the related Identity Business Processes with a role. In a majority of cases solutions bolt business process on top of resource centric roles/rules using ever more rules and making it difficult to truly understand and assure what is happening. More critically, it becomes a significant effort to change the underpinnings to deal with process change – which, as we

have just discussed, is the most significant component of any Identity Management initiative internal to an organization.

At one end of the spectrum we see the pure technology level approaches in standards such as SAML, SPML and a number of the WS-Federation initiatives. Moving along a step, we find the Liberty Alliance. Driven significantly by both technology and provider organizations, the Liberty Alliance acknowledges the challenge is not only technology, and is attempting to incorporate more business focus in their capabilities. However, they are still linking their business processes through point to point agreements that are only loosely confined, and have yet to be challenged by any legal issues. At the other end of the spectrum Ping ID proposes comprehensive legal and business environment for organizations to sign up to, and also defines guidelines for levels of trust and mediation in the event of a process failure.

**FIGURE 3: CROSS-ENTERPRISE FEDERATION – BASIC MODEL**



### Federating Processes vs. Federating Security

When federated identity maps identities across organizations, the reality is that we face the same challenges that we do internal to an organization. In fact, most internal federation efforts started at the data and process layer, and ended up requiring iden-

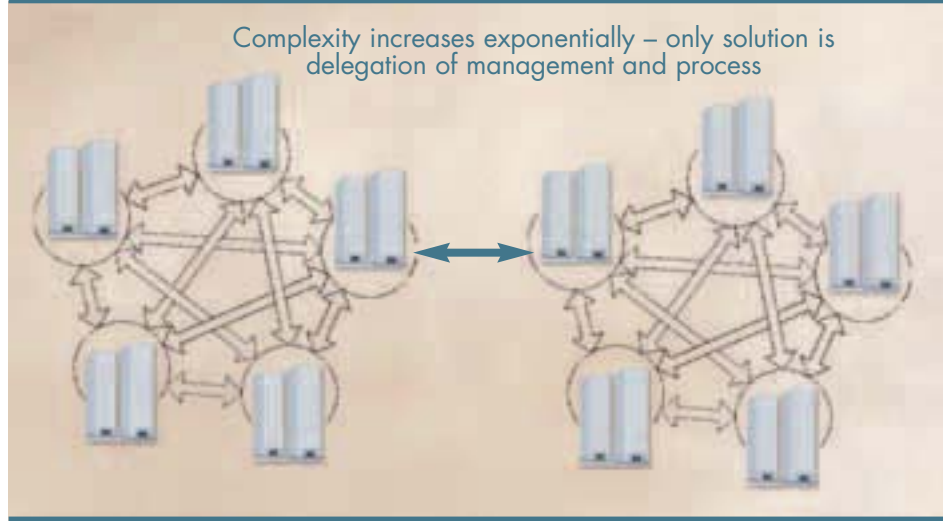
tity management to support the effort. External or Cross Enterprise Federation has started at the top layer, trying to automate moving credentials between organizations, and requiring that the process and data level integration occur.

This top down approach, however, is only scalable in a security model, not a process model. Mapping identities is not enough. Process integration is critical to make Cross Enterprise Federation a success, and the current crop of standards is only the beginning. The biggest risk, challenge and opportunity lies in the ability to seamlessly move processes across organizations.

For example, consider being able to define required processes that a partner must follow, passing those processes to the partner, having them executed, and returning a guarantee that they had done so. This would allow the first organization to create an auditable and validated trail that the process had been followed. Allowing organizations to take and run part of the process requirements allows creation of a scalable and secure deployment of federation. Furthermore this allows for the “delegation” of process control and execution. SPML is a starting point on the process story; however it is a long way from delivering on process interchange. Ping ID is at the other end of the rule, creating an environment where out-of-band processes can be agreed to and all parties in the process or transaction can undertake to meet the minimum level of process control on the understanding that there are penalties for not doing so.

In many cases, organizations may not have Identity Management in place, and may believe that before tackling external projects, the internal requirements must be completed to enhance understanding. Starting small and building from there is a significant contributor to the success of

FIGURE 4: CROSS-ENTERPRISE FEDERATION – COMPLEX MODEL



Internet standards. However, the risk/reward potential is much higher when we are dealing with Cross Enterprise Federation and thus, organizations should consider their historical process integration efforts as much as their identity management initiatives. This also applies when looking at an Identity Management solution, critically – can the same solution support both internal and external delivery of federation?

The DTCC profile article in the Mar/Apr Digital ID World provided a clear illustration of Extended Enterprise Federation. DTCC stated that their initial thought was to deliver internal Identity Management even though their pain point (in this case biggest risk and reward) was in their external. By being aware of their overall needs, they saw that specific solutions offered a way to solve both problems, while at the same time mitigating the risks involved. Now, because of the delegation capabilities that the DTCC have implemented both in terms of administration and APIs, there is a significant opportunity to grow their extended enterprise into a cross-enterprise federation. As other organizations implement Identity Management solutions that support the provisioning and process APIs provided by the DTCC, they can deliver a complex yet scalable Cross Enterprise Federation initiative.

### Summary

Current identity federation efforts are focused too heavily on security and tech-

nology, and in particular on scaling this part of the federation solution. This is detrimental to the critical function of business process integration, which turns out to be the major cost element.

The challenge when looking at federation is ensuring that the solution set can scale both in terms of the technology as well as the more costly process management. You should make sure that a solution can support both internal and external initiatives, allowing you to offer extended and cross-enterprise federation using the same business model, as well as manage web services. Few solutions currently support all levels of Federation. The Liberty Alliance is working to incorporate a number of the aspects discussed here, including the ability to extend trust across organizations and increase the speed of deploying federation. I would additionally recommend considering the efforts of Ping ID as the basis for any federation planning as well as their SourceID code libraries. A related work is the Global Grid Forum which grew out of Liberty's earlier explorations into trust models. ■

Archie Reed is Director of Strategy at HP and member of the Digital ID World Industry Advisory Board. He is the author of several books on identity topics including *Implementing Directory Services* (McGraw-Hill) and *The Definitive Guide to Identity Management* (Realtimepublishers.com).