

Identity Management HITS THE FAST TRACK

Identity Management began as a ponderous, heavy technology. But it has quietly evolved in many significant ways over the past two years. While each step by itself may seem small, together they have created identity management that is far less expensive, far more predictable and rapid to deploy, and capable of far more comprehensive solutions. These less invasive and more easily integrated solutions also allow staged, incremental deployment not previously possible. The days of “boil the ocean” identity management have passed. This evolution has quietly positioned Identity Management to hit the fast track.

It has taken a long time for most people to realize the central nature of identity as an organizing paradigm in networked computing. But even if that paradigm hasn't been fully recognized yet, the term Identity Management has emerged to focus the issues. We've largely passed through the period of “what's that?” and today most understand that identity management in some way goes beyond authentication, authorization, and administration (AAA) to create a more unifying administrative, management and security infrastructure, even if they may still not be quite clear how. And it is still the case that many remain limited by an outlook that sees Identity Management and Directory Services as essentially the same thing.

Identity Management deployments are increasing, and all analysts predict a breakout in market deployment in the next three years or less. The only remaining question is when will the inflection point arrive, and how big will it become. Interpolating analyst predictions, and adding a bit of

Digital ID World expertise to the mix, indicates that inflection point will occur in 2005, and that the size of the market it creates after that will be much larger than most analysts think. Why is this happening, and why now? It is because of a combination of increasing customer need and the evolution of identity management technology.

Crossing Thresholds

Infrastructure technology evolves slowly, and it is easy to miss those moments when it evolves past thresholds that change its usefulness dramatically. In this feature section, we highlight some of the more important evolutions in identity management, and provide you with perspective on why they represent a state change in the usability, deployability, reliability, and maintainability of the technology. At the same time, we shed some light on what has been learned in the real world deployment of identity management, and how field experience is affecting both the technology and the companies that manufacture and implement it.



In our interview with Mike Beach at Boeing, you hear from someone who has been in the trenches for successful pioneering identity management deployments – both internally facing and federated with external partners. And our deployment story relates the experiences of Fifth Third Bank, who deployed both enterprise and federated identity management from a standing start within the last year. Taken together, these two articles reveal a great deal about the evolution of identity management through the eyes of those who have deployed it.

Identity is an Architectural Thing

One of the biggest evolutions in identity management has nothing to do with the technology itself, although methodologies are changing as a result. It is the dawning realization that identity management must be addressed as an architectural issue, not as an application or security product deployment. We've written about that many times, but it seems to take experience to really understand what that means. Experience inevitably leads there, however, as all of these real world case stories reveal.

Our case story about Lehman Brother's provisioning deployment illustrates the importance of seeing the bigger picture of what you are doing as being business process focused more than technology focused. They had to learn how to engineer their business processes and deployment methodology so they could bring identity management to 300 applications per year. Ramin Safai, AVP of Information Security at Lehman, echoes most who have gone through an identity management deployment when he says, "it's all a game of process development."

Another theme you will see with identity management is the way in which experience with its deployment relentlessly makes you aware of boundaries you want to dissolve, and how much more it can do for your organization than you initially were thinking about. This is highlighted in the article "Identity Management Becomes Customer Driven," and is another indication of identity's essential infrastructural nature.

Things Have Changed Dramatically

When you read these stories, what becomes clear is that the evolution in identity management technology and perspective is relentlessly creating a very different landscape. Each change by itself may be small, but in the past two years the combined evolution has crossed many thresholds. "We have seen over the past couple of years as we've moved to new versions," said Boeing's Mike Beach, "that we have been able to eliminate customizations in favor of out of the box offerings that weren't there a couple of years ago."

This has happened for many cycles now, with the result that a new deployment faces far less custom integration than ever before. The evolution in agentless provisioning techniques, for example, has made provisioning deployment much less invasive than it once was. The rise in adoption of standards in many areas has created more open interface points than previously existed, again making things easier to deploy.

There is still significant work remaining, but the experience of Bob West and Fifth Third bank dramatically illustrates how much things have changed. The speed with which an entire identity infrastructure was stood up and deployed with both internal and federated identity is hard for those who attempted something similar a few years ago to believe. His experience demonstrates that it has become possible, but he also makes it clear that how you

understand and approach what you are doing is critical to success.

Uncoupling from "The Directory"

Tales of "Directory Projects" that bogged down and dragged identity management down with them abound. But if you listen closely, you'll realize you aren't hearing many of them any more. The reason is that new approaches, new understanding, and new technologies have refocused identity management on its real mission, and that doesn't require a single directory.

Our article on why "The Directory is No Longer the Center of Identity Management" explores another change in identity management. This change – from thinking the task was to build a single, unified identity store to realizing it is one of networking and managing distributed, networked identity stores – is one of the most significant that has occurred in the past few years. Archie Reed's "Do I need a Directory Strategy?" is the personal story of a directory advocate who has changed his perspective and why.

Understanding Centralized vs. Networked

Another realization has slowly worked its way into identity management technology and methodology over the past two years – that it isn't the identity data itself that needs to be centralized, but rather the policies that manage its administration and use. The understanding that if policy management is centralized nothing else needs to be has opened the way to significant evolution in identity management over the past two years.

The freedom from directory-centric thinking has allowed the commonalities of the administrative and execution policies to be recognized, and they are beginning to become integrated as a result. Another outgrowth of seeing identity stores as distributed and networked instead of centralized

is a new appreciation of the place of virtualization in identity management.

As with any revolutionary technology, virtual directories had to go through a learning and maturing curve, and their early reputation wasn't the best – to put it mildly. But as with the rest of identity management technology, they have evolved through field experience and matured. In the article “Identity Management Becomes Customer Driven” you will learn how virtual directory and provisioning are being combined to create a rapid identity store integration and cleanup capability – critical for rapid new deployments. Just one example of the impact this technology is beginning to have.

A Changed Landscape

The combination of the realization that the task is to centralize identity policy while networking the rest, and the evolution of

myriad new techniques to do just that has brought us to a place where a state change in identity management capability is occurring. The evolution will continue, and there remain many “round-plug/square-plug” standards issues to resolve, but we have reached the point where identity management is truly deployable, reliable, and maintainable without an army of service personnel.

A year ago this feature section was titled “How Identity is Refocusing IT.” Today it is those deploying identity that are refocusing Identity Management technology and vendors. The demand is being driven by the need to manage and secure networks at scale, and by regulatory requirements that companies enforce identity driven policies in networked applications, and pass audits that they have done so. The result is a slow, but definite shift from a security world-view to an architectural manage-

ment world-view. That is impacting how we see computing itself, as illustrated in Justin Taylor's article “The Business Case for Identity Driven Computing.” Here Justin lays out what is happening in networked computing and why it is relentlessly driving towards identity management as **the** management paradigm.

Identity Management products themselves have become integrated with more things out-of-the-box, and become far more flexible in how they integrate with what remains. They are changing their focus to centralize and integrate policy creation and use that to automate widely distributed self-service and delegated administration, compliance policy enforcement and auditing, and access management. We are seeing wide variations in how rapidly various vendors understand how to accomplish this, but all of them have moved onto the fast track with identity management. ■