



From the Editor



BY PHIL BECKER

Identity Management isn't so much a new thing, but rather a more coherent way of looking at what had previously been seen as many separate components. But that shift in perspective makes all the difference.

What do you think Identity Management is? On phone calls and at conferences I have been hearing this question in one form or another for the past few months, often asked by someone who it would seem should know. Identity Management has achieved full “buzz word” status, and every company that can is saying that their product does identity management. While this has caused the world at large to know that “something is going on” called identity management, it has simultaneously caused confusion about what exactly it is. That this question is asked by those who do indeed know at least something about the subject is an indication of the power that is released by “getting the picture” of identity and identity management right. It also indicates that they know the danger of not getting the picture right. This is a classic indication that a paradigm change is underway.

The Power of the Paradigm

The definition of the word paradigm is “the generally accepted perspective of a particular discipline at a given time.” The much over-used (and misused) term “paradigm shift” thus means a change from one “generally accepted perspective of a particular discipline” to a different way of looking at and understanding it. Paradigm shifts, however, don't just happen. Rather they are driven by agents of change. This makes sense when you realize that there is no need for a paradigm change to occur unless the current paradigm in a particular discipline no longer allows us to fully understand and deal with what is happening because of changes that have occurred.

Humans resist change, and they don't change outlooks that have worked for them unless they stop working. Thus paradigm shifts don't occur just because the “generally accepted perspective” of a particular discipline is wrong. An outdated paradigm can stay in vogue much beyond its time if it is a useful tool. For a new “generally accepted perspective” to form, not only does the old paradigm have to cease being useful or correct at some level, but there must also be pressure from one or more significant “agents of change” that the old paradigm does not address well. In other words, for a paradigm shift to occur the old paradigm must cease being as useful as it had been specifically because change is taking place, causing it to no longer provide us with the ability to cope with the effects of those changes.

Agents of Change

We are at just such a moment in the networked computer industry. Several agents of change have appeared to make the old paradigms markedly less effective. Organizations are wrestling with the challenges of managing secure access to information and applications that are distributed across a wide range of both internal and external computing systems, and integrating systems that took different and incompatible approaches in their design. Such integration is being forced by acquisitions and also by extranet integrations with business partners. It is also desired to allow new business methods and/or products to be deployed.

The networked use of technology is also creating an explosion in the number of users for systems – users from many different sources both inside and outside of the organization. Managing the security and accuracy of this rapidly expanding user base seriously challenges

old outlooks and methods. At the same time, businesses are looking for competitive advantage and growth opportunities by accelerating the speed of their processes, increasing dynamic integration across administrative boundaries, and other techniques to leverage the networked computing systems we have built.

Each of these forces of change requires more automation and distribution of decision making about who is allowed to do what with which data and applications both to speed up processes and to scale them to handle much large user communities. And for many enterprises regulatory compliance is simultaneously ratcheting up the need to know what happened in systems that are becoming increasingly dynamic, operating across administrative and security boundaries, and which change their actions based on users' needs moment-to-moment.

The existing paradigms allow us to deal with some of this change, but they are too slow, too restrictive and inflexible to really let us see how to embrace these changes and use them to the advantage of our computing systems and enterprises. Change has now proceeded far enough that a new paradigm (generally accepted perspective of a particular discipline) is needed, and intuitively people know that. Thus the questions about "what do you think it is?"

Identity: The Emerging Paradigm

Identity Management isn't so much a new "thing" but rather it is a new, more coherent and unified way of looking at what had previously been seen as many separate components. It is a new perspective struggling to become the "generally accepted perspective" so it can provide a new way to see and understand what is happening in networked computing. This uni-

fication of view began a bit before identity emerged as the term to identify it. The first major step on the road to understanding identity was the consolidation of categories that occurred with the introduction of the term "Triple-A" for the combination of Authentication, Authorization, and Administration. Coining the term Triple-A was a recognition that what had been seen as separate categories were really intimately related, since authenticating a user doesn't mean much until you grant that user permissions to access things. Administering this layer of infrastructure was also different in key ways from what had been seen before, especially as tasks became distributed in the network. Again, the Triple-A category acknowledged that. However, even as it advanced the perspective of what was happening, Triple-A still left out several key components of what is now becoming seen as Identity Management.

Understand Identity to Understand Identity Management

The term identity is now fairly generally coming to be seen as not just a user name and password, but rather the entirety of a user's (or object's) meta-data. Beyond even that, however, identity data starts to take on a dynamic management and/or controlling aspect as evidenced by how things like portals are starting to create dynamic views into an entire group of applications and data that differ based on the user's identity attributes such as role in an organization, and other contextual data.

Directory services have spent years trying to abstract this component of identity into the X.500 directory structure, only to prove that it is too hierarchical and thus not really quite matched to what people and organizations want to see happen. So even as the directory emerged as a paradigm (generally accepted

perspective of a particular discipline) for storage of identity, attributes, permissions, and abstracting such things outside of applications themselves, that paradigm's structure channeled thinking into cul-de-sacs that have missed many of the implications of networked identity management. The directory paradigm limited thinking about network identity by causing people to think in terms of building large, integrated, synchronized and centrally managed identity stores. These are correct for some applications, but totally incorrect for others. Thus one must move beyond this paradigm to see techniques such as virtual directories and federated identity which are essential to solving many identity problems.

Authentication and authorization are hard problems, so it is natural that paradigms developed that focused only on these areas of identity. Again, however, while those paradigms work for certain problems, they mislead people in other situations. As with the directory paradigm, it has taken time and experience in the field with problems that current paradigms don't solve very well to realize that a new way of looking at things (perspective) is required.

So What is Identity Management?

Identity management is thus many things, but mostly it is a way of looking at the entirety of the problem set of integrating and automating security, authentication, dynamic management of data and applications, making access policy portable within a network and more. It is a perspective that says that all of these functions are at their core about the identity of the person or thing using the computer system at the moment, and the policies put in place by the owners of the applications and data those users desire to access. Identity management is the paradigm that results from such a focus.

Digital ID World is published bi-monthly by Digital Identity World, LLC, 3100 Cherry Creek South Drive, Ste 1505, Denver Co 80209. Phone: 303-663-7317 email: Advertising: sales@digitalidworld.com • Letters or editorial: editor@digitalidworld.com • Advertising: Eastern Region call 401-351-0274; Western Region call 949-366-3192 or email enquiries to: sales@digitalidworld.com.

Subscriptions are available for \$59 in the US or \$89 outside the US. Controlled Subscriptions are available to those who qualify. To subscribe, please visit www.digitalidworld.com/magazine. Or call 303-663-7317.



In This Issue

In this issue, I have written an article that seeks to clarify identity management by dividing it into Identity Management, which is a set of techniques to manage and propagate identity data itself correctly, and Management by Identity, which is the use of that identity data to actually manage the processes and create and audit the desired results in networked applications.

The conversation around “what is identity” and “what is identity management” is what Digital ID World is all about. Identity encompasses many computing disciplines, from identification (including biometrics and smart cards), to access control, password management, identity management, trusted computing, RFID, and more. In each issue we present case studies that provide perspective and context by illuminating identity and identity management, along with commentary on the effects of viewing computing through the paradigm of identity.

In October we held the second annual Digital ID World conference, and it was an amazing event. A great thing about having a print magazine this year is that I get to re-live that event with the perspective of a bit of time to think about it. Among other things the conference demonstrated that the new paradigm of identity is taking root and providing benefits, even as it also showed how people are approaching identity slightly differently based on where they have been. My conference review article pulls together many anecdotes from that all-star assemblage that illustrate what identity is, why it matters, and how the picture of it all is changing. And there are some fun photos of the goings on as well.

This issue’s feature section focuses on identity in financial services. Financial services were early to many of these techniques, often before they had names. This has had

its pluses and minuses. The pioneers are definitely the ones with the arrows in their back, but they have a lot of good information to tell you if you can listen. In the feature section, for example, we examine American Express’s federated identity strategy and see what the Liberty Alliance is all about and where its specifications apply. We also examine how bringing identity management to Instant Messaging allows it to be integrated into an overall identity management and compliance regimen.

Payments systems, and specifically automating payments systems and bringing them into the network has been a field with many failures and a few spectacular successes. James Van Dyke examines what the characteristics are that make payments systems more likely to deploy, and how identity is related to that. Eric, in his unique style, examines how identity, and specifically federated identity, may cause a shift in payment systems so significant it could affect which type of companies are at the center of that universe.

Interoperability and open standards are a requirement for identity management to become distributed in the network, and we take a look at one such standard – SPML – in this issue. We went straight to the source, the chair of the OASIS TC, to get the story of how this standard has come to be, and where it is going.

A seminal event for RFID occurred in November when Wal-Mart called a meeting of over 120 suppliers and outlined the plans for RFID enabling all the products it will purchase. They had previously indicated they would require suppliers to provide RFID by January 2005, but this meeting was the moment when it “got real.” We take a look at “The Meeting in Bentonville” to see what it means for Wal-Mart and its suppliers, and also what it might mean for RFID technology in general.

Paradigms are all about perspective, so we close this issue with

an article on the continuum of federated identity. Federation is a hot buzz word these days, but it is rare to have its meaning laid out so clearly as is done by Roger Sullivan in this article. He identifies the various problem sets that federation is intended to deal with, and looks at which technologies are appropriate in which cases. He also examines the business structures that are driving federation.

The Identity Conversation

My goal with Digital ID World is to create a forum for the conversation that is always required when a paradigm change is underway. It is never so important that all parties communicate their thinking as when an industry is groping its way towards a new “generally accepted perspective” of its particular discipline to deal with changes that are overwhelming it. As I say constantly, this digital identity conversation works best as an interactive venture. I encourage all readers to let me know what you find important, what you would like to see more coverage of, and what you would like to see less of so I can serve you better. I am always on the lookout for case studies that provide perspective on identity in computing, as well as contributions from those who are working in the field. Please send those thoughts to me at editor@digitalidworld.com.

Finally it is a fact of life that the faster our readership grows, the more capability we will have to cover the digital identity conversation. So please pass this magazine on to anyone you think should be reading it, or give them one of those subscription cards you find annoyingly tacked into this issue. It will help us grow to be a better resource for you. ■



Article Reprints, Eprints, and NXTprints:
Increase exposure by including article Reprints, Eprints, and NXTprints in your next promotional project. High quality article Reprints, Eprints, and NXTprints are available by contacting:

REPRINT MANAGEMENT SERVICES
Toll Free: 800-290-5460
717-399-1900 Fax: 717-399-8900
Email: info@reprintmgt.com
Visit www.reprintmgt.com
to obtain quotes and order reprints online.