

The Business Case for Identity Driven Computing

BY JUSTIN J. TAYLOR



If you look closely, you'll notice that everything has a life cycle that requires management. Technology works to automate this management, but differences in management paradigms, standards, protocols and methods have created a chaos of multiple management structures. To bring order to this chaos, we have to redefine what we are truly managing. This leads to Identity Driven Computing.

I Identity. In the last few years, no other term in the computing world has been so controversial and had so much written about it. Conferences and magazines (such as this one) have mushroomed to cover the realm of digital identity concepts and technologies, adoption and developments. Everyone from technologists and academics, to philosophers and theologians have commented on the concept. While controversial in definition and nature, identity is an extremely vital component to computing.

This surge in interest in identity has taken something that was once the purview of the IT department and broadened its scope for business executives and company boards. The result has been strategic identity projects so businesses can get a handle on the growing need for managing the identities within and without their organizations.

Identity is not the only critical focus area for businesses. Besides deploying identity management solutions, companies have been investing in all sorts of other technologies in order to provide value to their establishments by providing increased agility. Some of these technology solutions – such as resource, server and network management – are mature. Others, such as grid and autonomic computing, Web service and service oriented architectures, are newer, sexier, and less mature.

All of these architectures and concepts are being designed, built and deployed for one reason: to bring order to the chaos of business. To begin our discussion let's examine where the chaos comes from.

Chaos from Complexity

Chaos is a result of complexity; complexity comes from scale; scale comes from growth and growth is what every business wants. To put it in the most straightforward way, complexity comes from success. Thus success can actually lead your business to get more complex, as it is a direct result of growth. To see why this is so, examine how company growth occurs.

As a company grows they get more customers, This in turn means that the company has to hire more employees. The company also buys or re-tasks digital devices – laptops, for example – in order to help employees get their work done. Each of those devices needs software to make them function. That software needs to be managed and patched, and so on and so forth. This constant life cycle of business is exacerbated by growth and can cause chaos within a company, which then translates into a financial burden and an impediment to future company growth.

Growth and success are not the only factors that make business complex.

Business is complex and the current methods of managing the complexity, while working today, will not be up to the task in the future.

External factors also play a part in compounding the complexity of business. What are these external agents of complexity? Regulations.

Regulatory Impact

Today's businesses have to deal with more regulations than ever before. In the United States alone we have killed entire forests to print the regulations – even more to print the explanations of those regulations as defined by experts, and the guidelines that auditors use to assess compliance. Terms like Sarbanes-Oxley, Gramm-Leach-Bliley and HIPAA are now not only part of the board room lexicon, but the IT department's as well – since in many ways they are responsible for putting them into effect. Besides having ever more regulations, the nature in which those regulations are implemented has changed in two key ways.

The first way regulations have changed is in the consequences for non-compliance. In the past, most regulations involved fines for non-compliance, as well as potential embarrassment for the company as their non-compliance was made public, resulting in consumer mistrust. Now, due in large part to high profile cases such as Enron, contemporary regulations involve not only embarrassment and fines, but criminal consequences for company executives. The result of this is that CxOs are more and more concerned with compliance, and want to have more hands-on involvement in the implementations that ensure compliance.

The second change involves the inclusion of technology in the regulations themselves, with some regulations actually specifying particular components

such as encryption levels or electronic auditing requirements. When you add in the need to deal with the heterogeneity, and contradictions of global regulations, the task becomes even more arduous. Together with mergers and acquisitions, unique line of business needs, security and trust concerns, governance issues and just plain old competition, we have reached a complexity zenith! How can we eliminate this complexity?

Gaining Order from Chaos

Complexity will never disappear. The best we can hope for is to keep the complexity from becoming chaotic – to man-

One of the unspoken realities about these systems is that they can each add a new layer of complexity if they become a new silo within the organization

age it and apply some level of order. From a computing point of view, companies deploy a variety of systems to help automate the life cycle of various business entities or assets. To add to this complexity, there are as many management systems as there are entity (resource) types in your business. Identity management helps manage user life cycles; resource management helps manage server, desktop and software life cycles; network management helps manage routers and switches, and document management helps manage documents.

One of the unspoken realities about these systems is that they can each add a new

layer of complexity if they become a new silo within the organization. That complexity stems from the unique paradigms these systems use to manage their entities. Think of this as you examine your own systems: some systems may use groups for management, others may be policy-driven, and still others take neither approach or utilize both. And when you ask why they are all different, you get an answer that typically includes the phrase “because each type of resource (entity) is different from the others and needs its own way of being managed.”

Maybe this is the whole problem! Maybe if we found the commonality between these so-called disparate resources we could find a way to solve the problem.

Finding the Commonality

Ralph Waldo Emerson once said “the ancestor of every action is a thought.” Written another way, “our thoughts control our actions.” As illustrated above, we need to change our thoughts around managing and designing systems to provide better integration and collaboration. A good way to begin is to find the commonalities between the systems themselves. So, what do they have in common?

The first thing they have in common is what they do – manage life cycles. All resources or entities in a business have a life cycle to manage. If you are talking about a person, you will hire them, provision them, handle their changes (promotions, moves, etc.), and at some point retire them. This same life cycle process applies to managing resources. You acquire a device, load the software, patch the device, patch the software, over and over again, until it is retired.

We have been trained to think of “identity” as meaning a person. But “things” or other business assets are identities too – everything from devices such as laptops, PCs, mobile devices to documents and even Web services.

If you look closely, you'll notice that everything has a life cycle that requires management. This realization alone, however, does not solve the problem. Differences in management paradigms, standards, protocols and just about everything else in each system still exist. We have to go one step further. We have to redefine what we are truly managing.

Expanding the Definition of Identity

At the 2003 Digital ID World conference in Denver, I began my quest to do just that in a session entitled, “Taking Identity Beyond Carbon Based Life Forms.” The premise of the session was that “things” or other business assets are identities too – everything from devices such as laptops, PCs, mobile devices to documents and even Web services. This hypothesis, as you can imagine, had some supporters, some pessimists and a few people wondering if I was in full control of my mental facilities.

Part of the problem with getting people to accept this concept is that they have been trained to think of “identity” as meaning a person. The dictionary even defines identity as the “distinguishing characteristics of a person.” But in the computing industry we can redefine anything we like, so let's rewrite the definition of identity to be “the distinguishing characteristics of an entity.” A small, simple change, but a pivotal one.

Replacing the word “person” with “entity” opens up new ways of thinking about identity, and allows for possibilities that were previously unimaginable. Here are some examples:

Authentication at the Device and Service Level. Security and trust are key aspects that require close attention. As we move toward service-oriented architectures and grid computing, it will become more important to begin authenticating and authorizing more than just people. Devices must be authenticated to systems, not just the person using the device. Services and applications must be authenticated and authorized in order to protect against viruses and spy-ware. Imagine grid computing as it grows over the next few

All of these architectures and concepts are being designed, built and deployed for one reason: to bring order to the chaos of business.

years without this capability – complete chaos as new forms of viruses are written to infect grids.

Policy-Based Management. Now that we're talking about authenticating and authorizing more than just people, policy-based management will be imperative to allow systems to intelligently make decisions. Policy-based management, a feature traditionally found in identity management systems that only manage people, will allow provisioning of services and devices and management of their respective life cycles in a truly dynamic fashion. Policy can also be applied at any level, not just the at the human level. Imagine being able to

set a policy that dictates which devices or types of devices can access certain files or types of data .

Integrated Work Flow and Self-Service. For those times when policy requires another process or a person to authorize an action, integrating work flow into technology can greatly simplify collaboration as well as allow people to request access to resources.

Identity Driven Computing

This new concept is called Identity Driven Computing – a computing model based on the simple, but revolutionary, concept that all entities in your business are identities. Identity Driven Computing allows technologies that have been created and tuned for people to be applied to many different types of assets. The ultimate goal is to create an autonomic computing environment that uses identity as the common denominator. Identity becomes the paradigm for the future.

Business is complex and the current methods of managing the complexity, while working today, will not be up to the task in the future. By leveraging identity as the common thread for making systems work together, we can begin building truly agile enterprises. What does the Identity Driven Computing architecture look like and how can your organization realize its full potential? That will be covered in our next article. ■

Justin Taylor is the Chief Strategist for Digital Identity in Novell's Office of the CTO and a Board Member of the Liberty Alliance.