

# Sun Expert Exchange

## “Enabling the Virtual Enterprise with Identity Management” Thursday, November 11, 2004

**Well (Q):** Do you think Directory Server is the best choice as repository of Role/Policy/Org/User for Access Manager ? Ever think about to use DB, like Identity Manager ?

**Don Bowen (A):** Directory is a good choice for identity data because it is tuned to handle the high volume of read traffic answering questions related to authentication and authorization. There is a database behind the Sun Directory, which is how we achieve better performance than our competitors, but it isn't an RDBMS. Identity Manager makes very good use of an RDBMS for its data but it doesn't have to handle the volume of real-time activity a directory does.

**Vikas (Q):** Where can I find Documentation and WP about Identity Management

**Tamara Rezier (A):** Have you had opportunity to visit: <http://www.sun.com/software/products/identity/index.html>  
Here you'll find a number of whitepapers, datasheets, guides, etc...

**PhilippaBA (Q):** Is it typically difficult to combine identity management from security perspective and the identity management that HR systems want?

**Naresh Persaud (A):** From a security perspective our solution manages the process and insures that employee changes in HR are reflected in access across the enterprise. We leverage HR systems as an authoritative source. In addition we provision to users to the HR systems based on their job roles. When the user separates from the organization we are able to capture the separation workflow and de-provision their accounts in a timely fashion to reduce risk of intrusion.

**wdh44 (Q):** What are the differences between LDAP and the Identity Manager?

**Sara Gates (A):** LDAP provides the repository for critical identity information. Sun provides the leading directory server on the market, offering out of the box services such as security, failover, load-balancing, web-based interface, synchronization with Active Directory. Identity Manager provides complementary capabilities, with automated user provisioning, password management, identity synchronization and audit & reporting across a wide variety of systems, including LDAP, mainframes, databases, packaged applications, etc. These 2 technologies each provide unique and significant value in an overall identity management solution.

**Well (Q):** Does Sun have PKI/Certificate Solution/Product ? Or suggest a 3rd party product ? Can it integrate with Sun's Identity Management product stack ?

**Don Bowen (A):** Sun no longer sells a Certificate Authority solution, but we do partner with Entrust and a few other vendors for this capability.

**Vikas (Q):** Who are your competitors in Identity mgmt.? and how are you better?

**Sara Gates (A):** We primarily see IBM in competitive situations, so they are our primary competitor. There are a few key areas where Sun outshines IBM. First, with our provisioning product, we introduced to the industry the first converged provisioning & meta-directory solution so that customers can manage all facets of an identity from a single solution. IBM, on the other hand, provides 2 distinct products - 1 for provisioning and 1 for meta-directory - which makes it more expensive and complex for customers to deploy and maintain. Also, Sun's Identity Manager led the market in offering agentless technology for managing identities, and IBM, on the other hand, still lags behind in bringing that non-invasive approach to market. This architecture is critical for customers as it speeds deployment times and eases ongoing management by reducing the amount of work required to get connected to systems on which identities need to be managed. Next, Sun provides the market leading directory server, providing the most secure, scalable directory on the market. With the last release of Sun's Directory Server, Sun introduced a number of new key capabilities that provide a complete directory service to customers. For example, Sun provides built-in security and proxy services, which provide load-balancing and failover capabilities which are essential to managing a directory infrastructure. Sun also provides a web-based interface for managing directory objects. Sun simply considers these part of an overall directory service - whereas with IBM each service that I mentioned would have to be purchased from a third party vendor and deployed separately. Sun leads the market in providing the most comprehensive directory service. Finally, Sun leads the market in its commitment to supporting open standards and cross-platform support - which are essential to customers.

**klpsys (Q):** What specific tools are available now to integrate MS Active Directory into an overall identity management solution based on Java System Identity Manager.

**Naresh Persaud (A):** In Microsoft environments we manage Microsoft resources better than other vendors We support AD, NT, Exchange, MIIS and the SQL Server platforms. From an adapter perspective there are a number of tools available. The first step in integrating is to auto-discover accounts from the target system. Each Microsoft

application adapter provides this capability. We also support the ability to batch process the information and for Active Directory we provide the ability to intercept password changes and synch across target resources. To provide continuous account management we provide a reconciliation feature that allows new accounts to be discovered and disputed accounts to be managed.

**JPDiaz (Q):** As a followup to my question about Identity Management as a business opportunity for Service Providers, I'd like to ask Jamie Lewis to discuss the liabilities of an Identity Provider Thanks

**Jamie Lewis (A):** The liabilities depend entirely on the type of transaction or business involved. Consider the case in which a service provider authenticates a person, and then asserts the validity of the identity for a business transaction. If it turns out that the identity was fraudulent, then the identity provider is in the position of having asserted the validity of a fraudulent identity. The degree to which that is a problem depends on what's at stake. If it's a credit card transaction, and the credit card company bears the liability for credit card fraud, then the liability could be low. If it's a high-value transaction outside of the credit card liability model, then the liabilities involved could be high. In any case, a provider needs to understand what the implications are up front and define how liability will be assigned, how dispute resolution will be handled, and how you will provide audit trails and logs to back up claims and assist in dispute resolution. Per some of the other questions on trust (see 16, 22 and 47), the enrollment and registration processes will be a big issue, and the more liability the identity provider assumes, the more rigorous those procedures must be.

**PhilippaBA (Q):** Dan Bowen said that Identity Manager is the first converged provisioning and identity data synch product. Is that within SUN or in general? What about the IBM Tivoli Access and Identity Management?

**Don Bowen (A):** IBM has two products. Tivoli Identity Manager, the former Access 360 product, does provisioning. Their IDI product does data synchronization. Two products, two different approaches versus one product.

**stephanie (Q):** Including them. It's frustrating enough trying to include them in the SunONE LDAP schema. Identity of resources has been our major pitfall.

**Don Bowen (A):** Not sure why schema would be difficult to add. It can be done over protocol, by editing schema files or by using the directory console. With more specifics maybe I can provide a more detailed answer.

**PhilippaBA (Q):** Where are the real hard benefits in Identity management? Is it mainly in password management?

**Gafar Lawal (A):** Password management is definitely a benefit. Especially if you consider the amount of calls the helpdesks typically field for password changes and management. However, we also get the following benefits: 1. Self provisioning of passwords, name changes and similar personal attributes 2. Single Point of Management - considering user date consistency and validation. 3. Administration of Business Rules and models in a simplified manner in contrast to the complex lines of code that's typically necessary to accomplish such from application to application 4. Enablement of federation with B2B partners using concepts like role mapping and transformation. I can go on and on. But in the interest of time, I can discuss offline if necessary.

**vgupta (Q):** In a scenario where I have both the Identity manager and Access Manager, who does the application (s) talk to? The access manager or the identity manager?

**Naresh Persaud (A):** In the case where you have both there are several integration points Identity manager will manage the roles and user accounts in Access manager as provisioning target . In addition Identity Manager can leverage Access Manager as a passthrough authentication target so that a user once signed on can seamlessly use Identity Manager. All other applications protected by access manager still utilize an Access Manager policy agent to authorize access. An important note is that Identity Manager can still be utilized to provision accounts to applications guarded by Access Manager.

**Wes (Q):** RE: "Do you believe Federated Identity will ever become a reality in the B2B space? Or is the level of business trust required probably too high?" Suggest: sound enrollment services will be required in order for there to be the required level of trust. Random HR employee ID issuance practices will not suffice.

**Jamie Lewis (A):** In short, I agree. Currently there really aren't any enrollment standards, as I said in my earlier answer to question 22. We've seen a few startup vendors focus on products that support enrollment, but none has hit the market quite yet. The degree to which enrollment becomes a crucial factor is, of course, dependent on the surety and assurance levels transactions require. Today, most companies are doing federated authentication (Web SSO) to B2B portals, and are leaving enrollment and accreditation up to the individual parties. In other words, we're crawling before we try to run. And we can learn from the work, and grow trust models in a more organic, business-driven manner. Wider circles will evolve through third-party services (such as market associations, etc.) Also, the US federal government's eAuthentication Partnership – which Burton Group has been involved in -- provides an interesting baseline on which we can start building wider circles of trust. (See <http://www.cio.gov/eauthentication/>)

**Illiad (Q):** At larger companies, is it best practice to have one group managing identity for all access channels (employees, suppliers, customers, devices, etc)? Or is a separation of power more efficient for implementation and

governance?

**Don Bowen (A):** Centralized management of identity can always achieve more economy of scale, but doing so in large organizations is rarely achievable. Companies who have been successful in deploying an enterprise directory have achieved better results in this area, but it really depends on the company. Trying to create a solution that swims upstream of the politics in the organization is frustrating. Ensuring that abuse of any aspect of managing identity isn't happening requires the right controls and audit process be put in place.

**Well (Q):** I heard that the #1 priority task in Sun/MS interop work is to solve Single Sign-On problem, what are the problem you guys have now ?

**Sara Gates (A):** We get a lot of questions about the Sun/MS interop work - so good question. Right now we are working on cross-certifying our products as interoperable so that customers benefit from our having done the work to make this easier for customers. For example, we are certifying Exchange on Sun's directory for high scale environments. In addition, Sun and MS are working to drive standards convergence in identity federation, as this will also benefit customers. Stay tuned for more on that.

**csaunderson (Q):** Could the analysts contrast the Sun approach against the trends in the industry?

**Jamie Lewis (A):** In short, Sun's direction is largely consistent with industry trends. Over the last three years, the industry has been consolidating through merger and acquisition activity. Larger companies have been acquiring smaller companies, and the general trend is toward suites of integrated identity management products. While there is still the concept of "best of breed", the concept has moved up a level; all product lines are now multifunction in nature. The strengths and weaknesses of the suites depend on a) where a given vendor's background and b) what companies it has acquired. Sun began from a directory background, and with its acquisition of Waveset, has been building an integrated suite of products, which is consistent with the trend Burton Group highlighted starting two to three years ago.

**Rob (Q):** Could you comment on the pros/cons of a meta-dir/synchronization approach versus a "provisioning" approach to managing distributed identity data?

**Tamara Rezler (A):** Our data suggests that 90% of meta directory implementations are identity-data (provisioning) related. Meta products had begun to add basic provisioning function. On the other hand, provisioning vendors already had the following: Multi-system, complex provisioning (account sync) Password Management, Roles/Policy, Auditing/Reporting, delegated administration and Self Service as well as a connection mechanism to push identity data to target resources. In order to accommodate managing distributed identity data, it was only a matter of providing the "pull" capability for identity data. So, if you have need for the functions listed, I'd suggest that a provisioning approach is the right one.

**Arsine (Q):** How does the System Access Manager integrates with different platforms like Cisco IOS, Solaris, Linux, Windows and custom made web applications for a centralized directory management? does it interoperate with other directory solutions as Radius, and RSA?

**Don Bowen (A):** Access Manager can be used by both web and non-web applications to facilitate a centralized authentication and authorization service. For web-based applications this is delivered by agents that run on the web server or app server. For non-web-based apps this is accomplished by using the provided SDKs. Integration with platforms like Cisco-IOS, Solaris, etc. are more of an ESSO solution and for this Sun has partnered with companies like Passlogix.

**Marsha (Q):** Are interfaces to other applications/systems built in, customized, or generic enough for implementations outside of SUN to install?

**Sara Gates (A):** Sun is committed to providing out of the box support for all leading applications and platforms on which identities need to be managed. Identity Manager for example, provides over 60 complete resource adapters that can be configured in a matter of minutes - from directories to databases to mainframes to packaged applications to - well, you get the idea. If custom applications need to be supported, we provide a Resource Adapter Wizard for configuring new connections.

**decksoft (Q):** the ROI for the case of ML makes sense (because their actual customers/services mass) will make the same sense for small business like us??

**Gafar Lawal (A):** If you consider that Identity Management helps in the management of the complexities of associating myriad resources to Identities that can span several categories. Then it should be relatively easy to see where it may not matter what the size of your company is in number of internal users, but the complexity of the size of your resources, assets, and potential clients. If you then add the ability to audit access and streamlining of administration that you get from a unified and converged solution, I think it almost becomes a "no-brainer"

**Well (Q):** Do you plan to include Identity Manager into JES ? I think the price is the major concern.

**Don Bowen (A):** There are currently no plans to add Identity Manager to the Java Enterprise System. Thank you

for the input on price. One thing to keep in mind is that Identity Manager is the first converged provisioning and identity data synchronization product.

**Wes (Q):** How can the user of a federated identity management system trust the identities of employees, contractors, etc. in a wide "circle of trust"? What enrollment standards can be relied upon?

**Jamie Lewis (A):** Currently there really aren't any enrollment standards. As I said in my answer to question 16, most federated deployments are working in pair-wise relationships today, not wide circles of trust. In these scenarios, federating partners are defining their own enrollment procedures, the levels of liability they are explicitly taking on (and disclaiming), and so on. In my opinion, the invention of a "global" trust model is, at least to some degree, putting the cart before the horse. In loosely coupled federations, trust can be pair-wise. Because federating parties today are already doing business with each other (see my answer to question 16), they can deal with these issues directly. And we can learn from the work, and grow trust models in a more organic, business-driven manner. Wider circles will evolve through third-party services (such as market associations, etc.) Also, the US federal government's eAuthentication Partnership provides an interesting baseline on which we can start building wider circles of trust. (See <http://www.cio.gov/eaauthentication/>)

**Illiad (Q):** Are there any successful projects using Identity Manager in conjunction with RFID? In what context?

**Sara Gates (A):** This is an emerging area of interest for customers, and right now customers are in the earliest stages of these projects. We believe the first focus of these projects will be around security and audit. Stay tuned for more on this.

**Erin (Q):** Hi and thanks for sponsoring this event. Do you have any data on what the overall opportunity for Identity Management Solutions in the Federal Government vertical may be?

**Tamara Rezler (A):** Sun has a very strong presence in the Federal Government. In fact, we have the only provisioning solution, Identity Manager, that has achieved NIAP's Common Criteria Certification. We are also the only vendor who have met requirements for ELA certification consideration. We have many federal agency customers including NASA and Department of Energy.

**vgupta (Q):** can I buy just the Identity Manager without buying the Access Manager?

**Don Bowen (A):** Absolutely. The Sun Identity Management "suite" includes three separate products. Identity Manager, Access Manager and Directory Server Enterprise Edition.

**qoslabs (Q):** what initiatives does Sun have to create and drive awareness of the identity management solutions with new prospects? Most customers are not aware of Sun's software solutions.

**Sara Gates (A):** We have a number of key initiatives underway to promote Sun's identity solutions. Stay tuned for more on that!

**PhilippaBA (Q):** Is roles based identity management really possible to achieve in a large organization?

**Gafar Lawal (A):** Merrill Lynch Global Private Client is a perfect example of such an organizations. We are in the middle of a rollout of this solution to over 600 branches with internal user population of over 25000. We have also role this solution out to support retail clients of approximately 1.5million. Again, I will be happy to discuss details of how we have accomplished this if you desire.

**Isham (Q):** What exactly is Virtual Directory ?

**A:** Simple answer: Virtual directory enables federating (aggregating) identity data from multiple heterogeneous sources like directory, databases, flat files, and web services - real-time - and makes it available to identity consumers via LDAP.

**PhilippaBA (Q):** Do you believe Federated Identity will ever become a reality in the B2B space? Or is the level of business trust required probably too high?

**Jamie Lewis (A):** While we are clearly in the early adopter phase of the market, federated identity is already a B2B reality. We estimate ~ 200 customers have implemented the Security Assertions Markup Language (SAML) for federated authentication (Web SSO) in B2B scenarios. Burton Group has worked with customers in financial services, federal government (the e-authentication partnership and GSA project), manufacturing, and other industries to get these projects going. You're right to point out that trust is a significant issue, which is why federation is occurring now, and will occur over the next several years, only where business affinities already exist. And usually in pair-wise relationships. Business partners, businesses and their customers (or suppliers) are already doing business with each other. In well-established business relationships, they (often) have existing contractual relationships that they are extending with agreements around federation. In other words, federation in which two companies that have never done business with each won't happen in the foreseeable future because of the trust problem. But pair-wise relationships, where both parties are already doing business and want to automate the process, make it more efficient, are great candidates for federation, and that's happening now.

**Rodolfo Bertoloni (Q):** Anybody could mention significant differences between Sun Identity Management and Oracle's Identity Management?

**Tamara Rezler (A):** Sun provides a comprehensive Identity Management suite that includes directory services, access management and provisioning and identity data synchronization services. Sun's suite of products are both integrated with one another as well as integratable. The latter means that we support heterogeneous environments - both from installing our products and provisioning to, so our customers can protect their existing infrastructure environments. In fact, we have a strong partnership with Oracle and support our customers' Oracle investments. We can provision to Oracle Applications as well as Oracle's RDBMS, in addition to many other target systems. On the other hand, Oracle's focus has been on providing an Identity Management solution really targeted to their applications and database platforms.

**SUNday (Q):** How is the V.E. implemented at Merrill Lynch?

**Gafar Lawal (A):** That's somewhat generic question. So I will do my best to answer this way. V.E. for Merrill - GPC, is approached from a holistic perspective that include re-architecting our business solutions using SOA metaphor. Of course the enablement of such an architecture requires a unified consistent and auditable RBAC solution with robust Identity Management. I will love to answer any specific question on how we have accomplished this at Merrill Lynch Global Private Client Business offline if you desire.

**Remi-AC (Q):** Is Identity Mgmt covering for access control to distributed systems with complex rules based on role, location, data restriction, etc? And is there any reference on the web specifically about this topic?

**Don Bowen (A):** Yes, Identity Management does cover access control to distributed systems and can handle complex rules based on role, location, etc. These capabilities are covered by the Sun Java System Access Manager product. You should be able to find information on this [www.sun.com](http://www.sun.com), but feel free to contact us with more detail if you don't find what you need.

**William Zhang (Q):** What is Identity Management, perhaps, Sun may give a brief overview.

**Sara Gates (A):** Sun sees identity management as a three tiered Identity Grid within the large enterprise or organization. The first tier is the repository tier where key identity information is stored. Much of the movement today, as you know, is moving to the directory-based infrastructure as the key repository for identity info. Sun has the market leading directory server providing this service. The second tier of identity management is the transaction layer, providing real-time authentication and authorization services, such as the web access management products. Sun has a leading product in this arena, Access Manager, which provides authentication, authorization and federation services. The top layer of the Grid is the Administration layer, providing provisioning, password management, user management, auditing, and identity synchronization. Sun has the market leading product in this segment, Identity Manager. These three components, the repository, the transaction services and administration provide the foundation for identity management.

**KJM (Q):** Do you offer integration solutions for Oracle Databases? Is it native support?

**Tamara Rezler (A):** Yes, Identity Manager provides a resource adapter to provision to Oracle ERP applications as well as the Oracle DB (8i, 9i and 10g.) The resource adapter is agentless, however we do support native drivers in addition to platform independent drivers.

**Philippa BA (Q):** What successful identity management projects have the panel seen? Was there a real ROI found post implementation?

**Gafar Lawal (A):** At Merrill Lynch Global Private Client, We have successfully deployed Identity Management as a component of an Integration Framework using Role Based Access Control as a framework for Security and Identity Management. our solution has been in production for over a year. The ROI is being quantified right now. However we see significant ROI on convergence of Identity across over 600 retail branches and decommissioning many legacy and sometimes hard to manage environments and data cleansing.

**Well (Q):** I'd like to ask Identity Manager and Access Manager guy. What is the pro/con of agent based architecture and agentless based architecture. These two product use completely different approach to solve problem.

**Jamie Lewis (A):** In theory, the agentless architecture is easier to deploy. In practice, however, this isn't an either/or question. Some end systems simply don't have robust enough, or even formally defined, APIs to support fully agentless provisioning. Burton Group believes that effective products must support both architectures, giving implementers the flexibility to choose the right approach in a given application context.

**moon (Q):** Hi, we plan to incorporate Identity Manager for our clients and want it to work with Active Directory. I find it difficult to find all the resources, etc to accomplish this. Is there some repository that has everything in one place, and or a guide that list everything you need from start to finish? Thank you.

**Tamara Rezler (A):** In Microsoft environments we manage Microsoft resources better than other vendors We

support AD, NT, Exchange, MIIS and the SQL Server platforms. While we don't make a central repository available to the general public, we do have numerous resources for customers and certified Sun iForce partners.

**JPDiaz (Q):** Hi Do you see an opportunity for Identity Management in Service Providers i.e. as a service offered to external users from an Internet Data Center, for instance. Thanks

**Jamie Lewis (A):** In theory, I think service providers have an opportunity as an identity provider. In practice, it depends on what kind of SP, and what you mean by opportunity. If by "opportunity" you mean "opportunity to make money," then I think there has to be a real business model/value proposition from the external user/customer point of view. We have seen mobile/wireless service providers, who have a built-in mechanism for billing and payments, work well with service providers of many types, which puts the mobile provider in a good position to have real opportunity as an identity provider. But in any case you have to be careful to understand the liabilities involved taking on the role of an identity provider.

**mike (Q):** Can the System Access manager use the Active directory?

**A:** As part of our increased interoperability with Microsoft this is something we will be delivering in an upcoming release of Access Manager.