

---

# **The Value Proposition**

---

## **Integrating Human Resources Enterprise Applications With LDAP Directories, Single Sign On and Identity Management**

Derek Small, President, Nulli Secundus

Guy Huntington, President, HVL

---

# Application Specific Directories

---

- Enterprise software vendors controlled access to their applications through a combination of vendor specific tables of user ids and passwords linked to business processes
- These are commonly known as application specific directories
- Only the enterprise application had easy and safe access to the information

---

# Application Specific Directories

---

- HRMS vendors implemented security with a view that HRMS application professionals would mostly be using the modules in a centralized manner
- Application use was therefore limited to a core number of “power users”
- Other applications such as e-mail systems, web applications and network resources also required this “people” data only resident in the HRMS tables

---

# Customization

---

- Companies that tried to implement employee self-service and manager self-service were faced with a significant amount of customization and administration due to the centralized design of application based directories

---

# Application Specific Directories

---

- Very costly administrative overhead to provide security for simple employee self service
- Every time an employee was hired, fired or had other status changes, security had to be manually modified
- There had to be a better and easier way of making this information sharable amongst ERP products and company applications

---

# Without an LDAP Directory

---

- The HRMS directory people and roles was not easily sharable with other applications
- Often would lack required data to support non-ERP applications
- Other applications had to first gain permission to access the HRMS directory which was often difficult or impossible to obtain

---

# Without an LDAP Directory

---

- HRMS had to open up access to the sensitive employee data for use by other applications
- Other applications requiring employee tombstone data are:
  - E-Mail Systems - Microsoft Exchange, Lotus Notes etc.
  - Work-flow Applications
  - Network administration - Need to create/expire network Ids
  - Network Security - Need people Profile for authorizations
  - Facilities Management - who, where, what and when
  - Telephony Support - white pages, cell phone possessions

---

# HR Questions

---

1. How do I securely share SOME employee identity information such that the information is secure?
2. How do I ensure that the information is provided to only those who need to see it?
3. How would I know that the HRMS is the authoritative source for that information?
4. Do I need to have everyone accessing my HRMS to do obtain this data?
5. I don't want my HRMS to be responsible for storing temps and contractors...how do we handle this?

---

# LDAP: “Application Glue”

---

- LDAP (Lightweight Application Access Protocol) is the “application glue” you need to bind together ERP components as well as non-ERP applications
- Each ERP component can “publish” and “subscribe” data to a common repository similar in concept to a tombstone identity vault

# “Gluing” Applications

- Human Resources can publish:
  - Employee status
  - Position Title
  - Reports-to relationships
  - Department Information
  - Participation in Benefits Programs
  - Locations...geographic, payroll, mail-drop etc.

# “Gluing” Applications

- Financials can publish:
  - Cost centers
  - Approval limits
  - Purchasing limits
  - Delegated authority time tables
  - Cost center relationships (roll-ups)

# LDAP Directories

- Other ERP components (Financials) needed to be linked to the HRMS component.
  - An LDAP directory provides an easy common point of focus and access to all applications
  - LDAP is designed for securing and bridging web-based applications
  - LDAP is standards driven and extremely optimized for reading data (they are really fast!)

# Defining Rules for Roles

- Network Operating Systems
  - Authentication
    - Utilize LDAP for definition of user identification
  - Authorization
    - Use LDAP for definition of user rights to use network applications and resources
  - Auditing
    - Use LDAP for tracking authentication and authorization at whatever level of granularity is required

# Defining Rules for Roles

- LDAP is designed for securing and bridging web-based applications
  - LDAP is structured to support the use of policy servers which define the business rules for authorization through applications such as Oblix's "Netpoint"
  - LDAP manages the use of certificates, biometrics, tokens, smart cards and digital signatures via Netpoint

# LDAP Provides....

- Definition of Internal Role Based Security
  - Human Resources and Financial information is often a component of defining an individual's role within an organization.
    - Derek is the Manager of Applications Development with \$225,000 spending authorization
    - Derek's manager for secondary sign-off for amounts > \$225,000 is Guy, the Director of Information Technologies

# LDAP Provides....

- External Role Based Security
  - Vendors require access to Accounts Payable applications based on:
    - The external role definition that is maintained in the directory identifying the user as having appropriate authorization for access to Vendor Portal
    - Delegated administration of the role provides the vendor ability to manage who within their organization is assigned to this role

# Why Won't This Work Without a Directory?

- Too complex and too many contacts to administer
- People administering the process have to know the security policy for the whole organization, the business processes and how they interact
- Administrators need to be notified in a timely manner
- Prone to error, time lapses and significant labor costs to keep information up to-date...poor security, poor entitlement and asset management

# Why Won't This Work Without a Directory?

- Application Directories Lack:
  - Standards
  - Speed
  - Scalability
  - Security
  - Ease of Access
  - Completeness
  - Ability to be partitioned or distributed

# The Result?

- Most enterprises don't have well maintained and automated security for internal applications
- Most enterprises are reluctant to provide access to external organizations for fear of the associated exposure
- As a result, many enterprises don't even implement manager/employee self service or, customer self service

# HR/LDAP Integration

- Real-time or near-time population of data that role definitions require
  - E.g. If Guy's position, title, job code, department, location, salary/grade, company, business unit change in the data base, then these can be populated out to the directory on a scheduled basis

# HR/LDAP Integration

- The directory is queried to determine if a “universal” identifier exists for the new hire
- Once hired, an ERP application ID is created and published to the directory or the existing identifier is retrieved

# HR/LDAP Integration

- As a new hire, when you sign onto PS for the first time, it will force the employee to change their password, go out to the directory and use a series of pre-defined business rules to generate a security role for the new employee
- The employee automatically has access to the application based on their new profile

# HR/LDAP & New Hires

- The network security system, firewalls, domain servers and web-servers will also be aware of the new hire since the profile is now active in the directory
- The e-mail system, which relies on the LDAP directory, can automatically create an e-mail identifier or activate the one created by the new hire process
- The voice mail system can be automatically updated based on the contents of the directory

# LDAP/Self service portals

- Use directories for employee and manager self service portals
- Assign rights based on the security role
- No longer have to create a series of web pages that are manager or employee centric, they all now come pre-shipped
- If you don't use LDAP, you can still do this by the application using filters that run against the database

# Without a Directory...

- To date, companies have been finding it difficult to create, use and maintain a common access point for people information
  - People info includes people on contract, not necessarily employees who are not placed in the HR database
  - It's difficult to keep security for network, building, telephony, IT hardware, facilities and the employee population in general informed of people coming and going

# Without a Directory...

- Creates security lapses as terminated people leave the company
  - Lost productive time as people enter the company and don't have access to the building, floors, systems, parking, they need to do their job
- Makes people less productive because they're not aware of who works where and who's responsible for what
  - Hard to find current organizational views of the company

# HR Keepers of the Data

- HR has been historically targeted as the keeper of the information
- Philosophical, tax and legal issues have prevented HR from maintaining the information in the HR database

# HR Keepers of the Data

- HR may not want to manage non-employees
- HR is unwilling to have network security and all sorts of other systems or people in the organization directly accessing the HR database to get this information

---

# That's Why LDAP!

---

- Easily accessible, standards driven, web based, information repository
- Directory can be the consumer of the information
  - HRMS databases feed HR information to the directory where the HRMS is the authoritative source

---

# That's Why LDAP!

---

- Directory can be master of the information
  - All non-employees such as contractors might be placed in the directory with the directory as the authoritative source if they don't reside in the HRMS
  - E-mail addresses, network privileges, facilities, telephony, building security, application privileges, parking, organizational information (who reports to whom), and geographic info. can all be mastered in the directory and replicated accordingly to the other systems

---

# Identity Integrity

---

- Answers old problem of how to create a single way to identify an individual in the organization that all systems can feed off of
  - Identity profile information is kept in the directory for all systems to interact with
  - Reduce redundancy of people information kept within the organization

---

# Single Sign On

---

- Using single sign on and identity management products like Oracle and Sun, the directory can act as the enterprise's coordinating hub for authentication using whatever authentication schemes the enterprise deems appropriate
- Directory can pass off authorization to PeopleSoft for ERP applications
- Directory can coordinate non-ERP authorizations

---

# Identity Lookups

---

- The identity management products can take position and org chart information from the HRMS via the LDAP directory, coordinate with other identity information and provide identity lookups via the intranet or extranet with simple point and click interfaces
- Identity information provided can easily be tailored to meet enterprise security policies

---

# Portals and B2B's

---

- Directory can help coordinate identity information
- Using single sign on products like Oracle and Sun you can use the directory and the HRMS to delegate both security policy and/or identity management to whatever levels make business, management and security sense

---

# Directories

---

- Infrastructure glue
- Knit together the various ERP components along with non-ERP applications
- Enable self-service features with security and ease of management
- Significantly enhance productivity

---

# Directories

---

- Leverage role and position management
- Enable single sign on
- Standardize security enforcement
- Coordinates identity information with the HRMS as authoritative source where you desire it

---

# I'd Like to Learn More!

---

Guy Huntington, HVL:

- [Guy.huntington@authenticationworld.com](mailto:Guy.huntington@authenticationworld.com)
- [www.authenticationworld.com/single-sign-on-authentication/](http://www.authenticationworld.com/single-sign-on-authentication/)
- 604-921-6797

Derek Small, Nulli Secundus

- [derek@nulli.com](mailto:derek@nulli.com)
- [www.nulli.com](http://www.nulli.com)
- 403-270-0657