
Integrating Single Sign On and Identity Management With PeopleSoft

Derek Small, President, Nulli Secundus Inc.
Guy Huntington, President, HVL

Background

- Today's operating environment requires information to be securely and rapidly interchanged between customers, employees, contractors and business partners via tightly integrated systems operating to web standards
- That creates many challenges...

Challenges

- Most systems weren't designed with tight integration in mind
- Some of the information to be exchanged is highly sensitive
- There's a lack of security standards and streamlined security processes between internal and external systems

Identity Information

- These challenges are especially noticeable in managing information about identities
- Many enterprises have come to the conclusion there needs to be some kind of high level identity coordinating hub within their enterprise and between enterprises

Examples of Need

- Coordinating high level or summarized CRM customer information with other systems
- Personalizing a customer, employee, business partner or vendor experience with a portal or web site
- Managing and using a company phone directory
- Coordinating company e-mail
- Finding office locations and floor plans

Examples of Need

- Managing identities in network management
- Determining employee positions
- Creating organization charts
- Managing contractor information
- Managing vendor and/or supplier information
- Finding general contact numbers/contacts
- Managing security identity cards

Enter LDAP Directories

- Many enterprises determine that use of Lightweight Directory Access Protocol (LDAP) directories is desirable to act as that coordinating identity hub
- PeopleSoft users often raise a number of questions at this point...

Key Question

- Instead of a directory, why not use the PeopleSoft HRMS product to store and support all this data?

Non-HRMS Data

- You could use the PeopleSoft HRMS database since it supports a few of the fields normally found in a directory
- The information required to support phone directories is scattered amongst a variety of tables and would also need to be augmented with additional “people” data not really required by the HRMS application

Non-HRMS Data

- This means modifying or customizing your PeopleSoft application that probably has too many modifications already!

Contractors

- However, the biggest concern many people have is the fact that most contractors are not in the PeopleSoft HRMS or Financials systems as users of the applications
- Maintenance of the identity information in the PeopleSoft specific security tables is very costly to perform and better managed by the LDAP directory which now talks to PeopleSoft

High Speed Access

- HRMS applications normally reside in Oracle, DB2 or other such enterprise databases, which are not geared to high-speed accesses required of phone directories and authentication processes
- Additionally, many applications such as network/application specific security and single sign-on require similar access to this data in a non-proprietary format that is fast to retrieve over IP

Authoritative Source

- That's why most enterprises are developing a strategy of using the HRMS as the authoritative source of employee data and then updating or publishing this data to the enterprise LDAP directory or directories for general consumption

Authoritative Source

- The addition of contractor information and other data related to pass cards and such are then maintained in web-based LDAP SSO applications such as Oracle and Sun

Portal Security?

- Why not use PeopleSoft security to manage the portal(s)?

Portal Access Security

- Access to PeopleSoft applications via the portal is very secure
- Accessing the portal via the Internet is not secured via PeopleSoft's application, as you have to be in the Portal to invoke the security layer
- Also, other non-PeopleSoft applications invoked from the Portal do not fall under the PeopleSoft security layer

Portal Policy Manager

- Thus the need for a policy manager that securely provides control to and from other applications in the Portal and to the Portal itself
- This is what Oracle and Sun single sign on solutions provide

Single Sign On

- By using the content of the LDAP directory to store policy for authentication and authorization, you provide a centralized control point prior to the user accessing the web-page or back-end non-web application
- Single sign on helps with the synchronization of identity information found in the directory and used by other applications

PeopleSoft vs. Identity Management?

- How do PeopleSoft and Identity Management differ?

PeopleSoft vs. Identity Management

- Beyond the obvious of one being an HRMS and one being a LDAP based provisioning and web-security application, they differ a lot
- In common, they both have data about employees, with the HRMS being the authoritative source for this data
- But beyond that, Single Sign On is a better repository of data about groups of employees and non-employees together

Coordinating Hub

- The key here is that you can maintain all “people” data and object data such as offices and floor plans associated with people in Identity Management for general consumption by the enterprise,
- Single sign on can support authentication schemes that provide differing methods of knowing who a person is in a variety of roles or circumstances e.g. certificates, username/password, smartcards, tokens, biometrics, etc.

Single Sign On?

- Our enterprise wants to move to a single sign on solution for most applications. How do PeopleSoft and the single sign on vendors fit into this?

Easy to Configure!

- Single sign on products like Oracle and Sun are easily configurable for single sign on out of the box
- This includes setting it up for use in multiple domains, different types of encryption and, as mentioned before, for different types of authentication

Post Authentication

- After central authentication, PeopleSoft will accept the authentication from the single sign on product and proceed with it's own authorization
- With single sign on products, it's also easy to configure it to send enough information after authentication to other applications such that the user doesn't have to sign on again

Reduce Costs

- Identity management products can provide easy and current view of all “people” data without having to maintain costly security profiles for PeopleSoft
- Information is available over the IP network, thus you can use the Internet for use in controlling access to your web-based applications as well as your non-web-based applications through the identity management product

Non-PeopleSoft Authorization?

- PeopleSoft will handle it's own authorization for single sign on to PeopleSoft applications. However, a lot of my other non-PeopleSoft applications are older and have poor or little authorization. Also, I want network and e-mail ids established or expired as employees come and go. Can single sign on help?

Yes!

- Authorization rules can be easily built and applied to other applications and/or web resources using single sign on products from Oracle and Sun
- It's not uncommon to leverage the use of roles and positions from the PeopleSoft HRMS to do this

Leveraging PeopleSoft

- The HR module becomes the authoritative source for the employee's position or role which is then replicated out to the directory
- The single sign on product then uses this information to see if the employee's role or position meets the authorization requirements for a non-PeopleSoft application or resource

Identity Lookups?

- Finding people, their contact information and position in an org chart is expensive to manage, time consuming, often out of date and frustrating
- How do I use PeopleSoft and identity management products to do identity lookups of employees, contractors, business partners' employees, etc?

Solution!

- Identity management products from Sun and Oracle uses easy to configure and install drop down search boxes that can be easily integrated into your intranet or extranets
- The search boxes take the information, query the directory and then display it in the intranet or extranet browser

Solution!

- The information being displayed from the directory is filtered by the identity management product as to who the administrators determine can view it
- PeopleSoft is usually the authoritative source for the employee information displayed
- Other applications may be the directory's authoritative source for contractor, business partners' employees or customers' information

Solution!

- Sun and Oracle identity management products can provide dynamic online org charts drawn from the PeopleSoft information such as name, title/position, direct and indirect reports

Position Management?

- Is using PeopleSoft Position Management key to using both PeopleSoft and identity management?

Position Management

- No, it's not really the key to success of such a combination
- In many cases you can employ differing approaches to derive reporting relationships, roles, routings and access rights based on a number of different data sources other than position
- Obviously using Position IDs and descriptions makes life considerably simpler, but it isn't a requirement of successfully implementing the integration

Important Note!

- Having no reporting or structural information in PeopleSoft is very cumbersome for PeopleSoft and really limits how well you can employ an enterprise directory
- We can help you with evaluating this type of assessment
- So far we have only found one client in our years of experience that didn't maintain any reporting structures in PeopleSoft. They eventually changed this when they started their upgrade to version 8.

Examples of HRMS to Directory

- Employee Identifier used in the HRMS and on Identity cards
- Employee work location – City, State, Building, Floor, Office
- Employee payroll location – ditto
- Employee Position Title
- Employee Job Title if different from Position
- Employee Department Description
- Reports to Position
- Reports to Manager Identifier

Examples of HRMS to Directory

- Indirect Reports
- Departments that report to the employee
- Employee status – (Active, Leave, Terminated, Retired etc.)
- Employment Type – (Contractor, Temp Part-time, Full-time, Temp Full-time etc.)
- Emergency Contact Information – (Spouse, sibling, brother sister etc.)
- Home Address Information

Examples of Directory to HRMS

- E-Mail address
- Phone Numbers – Home, Office other
- Address Information
- Work Location
- Reports to Information
- Indirect reports Information
- Administrator (secretary)

I'd Like to Learn More!

Derek Small, Nulli Secundus

- derek@nulli.com
- www.nulli.com
- 403-270-0657 (ext 20)

Guy Huntington, HVL:

- Guy.huntington@authenticationworld.com
- www.authenticationworld.com/single-sign-on-authentication/

604-921-6797