



Leveraging PeopleSoft HCM as an Authoritative Source for Identity Management and Provisioning with a Virtual Directory

Introduction

For most enterprises, the human resources system represents a vast and authoritative repository of authoritative data about employees, contractors and other human capital. In many cases, PeopleSoft HRMS is the starting point for employee identity, and so is a natural authoritative source for not only the identity of an enterprise's human capital, but also much of the context surrounding that identity. By leveraging the data inside of Peoplesoft HRMS, functions such as web single sign-on, entitlements, profiling, and provisioning can more effectively define and enforce policies that reflect the way the enterprise really does business.

PeopleSoft's LDAP interface is an excellent way to begin opening up HRMS data to these types of applications since most expect this type of data to reside in an LDAP enabled directory. It is also a double-edged sword: The more useful the data, the more attributes will be required, and the more synchronization will be needed to provide those attributes to the relevant applications in a format that they can easily consume them. A more effective way to quickly open the system to the many possible consumers of this valuable information is to turn Peoplesoft HRMS into a publisher of data. In this way, the owners of the data can continue to manage this data and control how it is presented to the rest of the enterprise from the perspective of security, privacy, and data accuracy while still providing the performance, high availability, and flexibility that these functions require.

Moving into the future, an eventual evolution of the PeopleSoft suite toward a separate and externalized identity management and provisioning system, like Oracle's Identity Management platform, offers considerable promise to address the above challenges cohesively. However businesses that have current PeopleSoft installations need a solution that can be applied today, without disrupting their current operations.

In this white paper, an alternative path to identity management and provisioning with PeopleSoft HRMS systems is presented, utilizing Radiant Logic's virtual directory solution. The core capabilities of this approach have been successfully demonstrated in a recent Proof of Concept jointly conducted by PeopleSoft and Radiant Logic. The next section provides a brief overview of virtual directories in general, and Radiant Logic's offering in particular. This will be followed by a description of the PeopleSoft-Radiant Logic Proof of Concept. The last section will re-state the case for this approach, in light of the Proof of Concept results and future directions.

The Virtual Directory

Virtual directories provide dynamic access to source data, serving up flexible, standards-based (e.g. LDAP) views in real time. This approach leaves the data in

place, preserving data ownership, while offering a layer of abstraction that handles all the complexities of multiple application requirements, such as on-the-fly transformations, granular security, data operation routing, caching, and load balancing. Data from disparate sources can be dynamically joined, creating new entries that don't exist in any data store. In addition to joins, entirely new attributes can be added to a virtual view, without the need to modify the underlying data schemas. This greatly accelerates new application development, and also reduces risk, since the data stores do not need to be changed. All of these features are focused on delivering all-important *context* to businesses, in a secure, highly available fashion.

Radiant Logic's virtual directory solution supports multiple formats to address most any identity-oriented need. In addition to handling standard LDAP, DSML, and HTML transactions, Radiant Logic's ability to process SPML and SAML extends the virtual directory to the provisioning and web services world, while providing support for federated security. Virtual modeling can reveal hidden relationships between data, expose orphan records, and reconcile information between separate systems. High performance caching, and intelligent synchronization services are available, leveraging well-established Java Messaging Service technology.

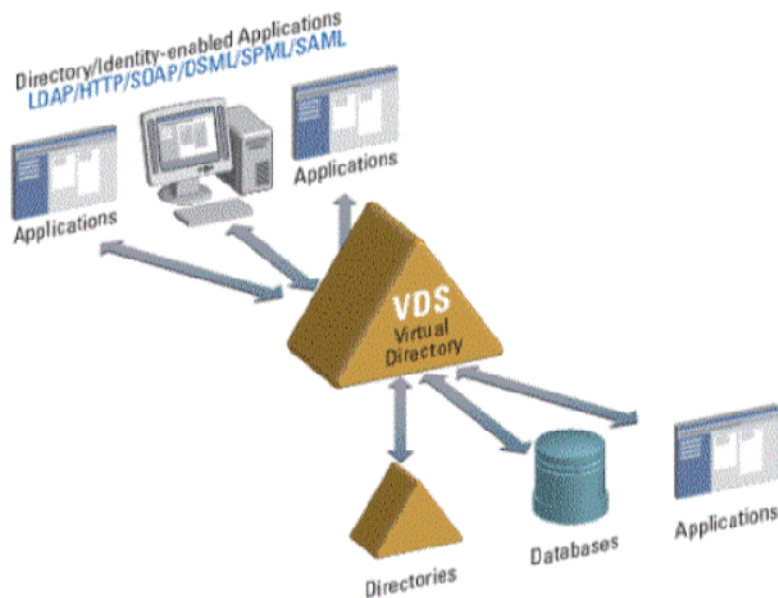


Figure 1 – The Radiant Logic Virtual Directory

Proof of Concept: Virtualizing Selected Information from PeopleSoft HCM

The Proof of Concept (POC) conducted by PeopleSoft and Radiant Logic, focused on four main operations: 1) PeopleSoft HRMS schema extraction and refinement; 2) Virtual view modeling and design; 3) LDAP authentication and authorization

delegation; and 4) Virtual view lookup from external system (PeopleSoft Financial application). The following diagram illustrates the high level architecture of the POC.

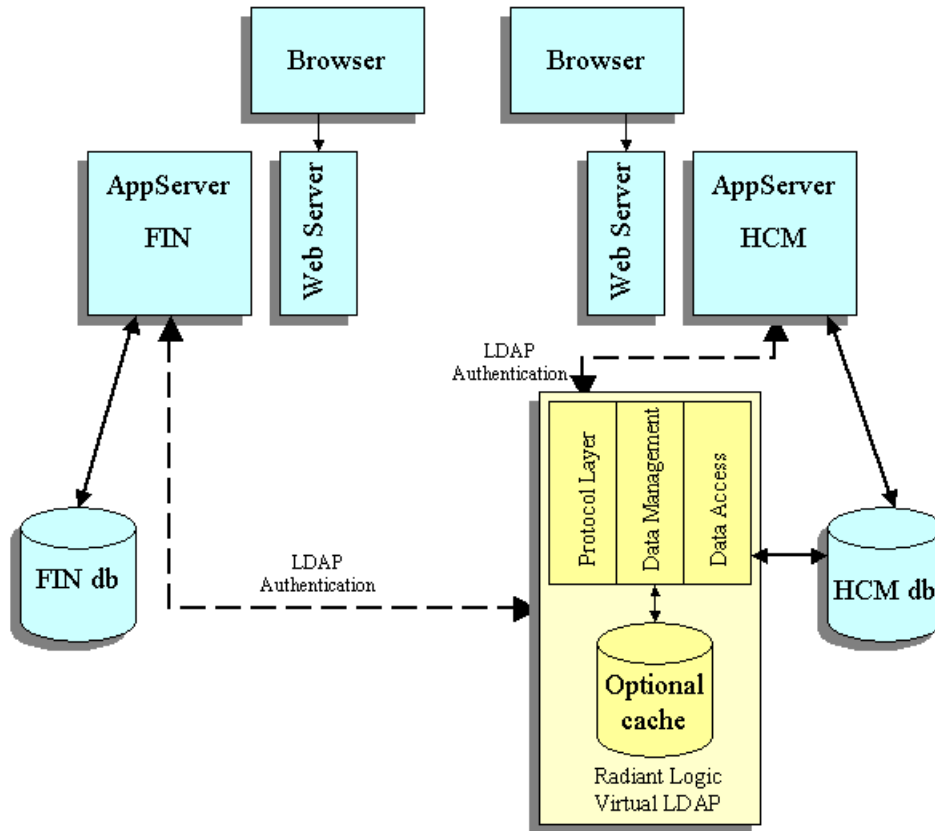


Figure 2 - High Level Architecture for PeopleSoft-Radiant Logic POC

Schema extraction. PeopleSoft HRMS consists of thousands of tables. A focused subset of tables was selected for the purposes of the POC. The selection criteria was based on a scenario where a PeopleSoft Financial application user requires employee identity data contained in the HRMS database.

Radiant Logic allows primary keys and relationships to be defined, even if they don't exist in the source data. Since no primary key was declared in any of the tables, EMPLID was declared as the primary key in Radiant Logic, and used to create several relationships between the selected tables. The primary key and relationships exist only in the virtual server – no source data was changed. The following diagram illustrates the extracted schema, and new relationships based on the EMPLID declared primary key:

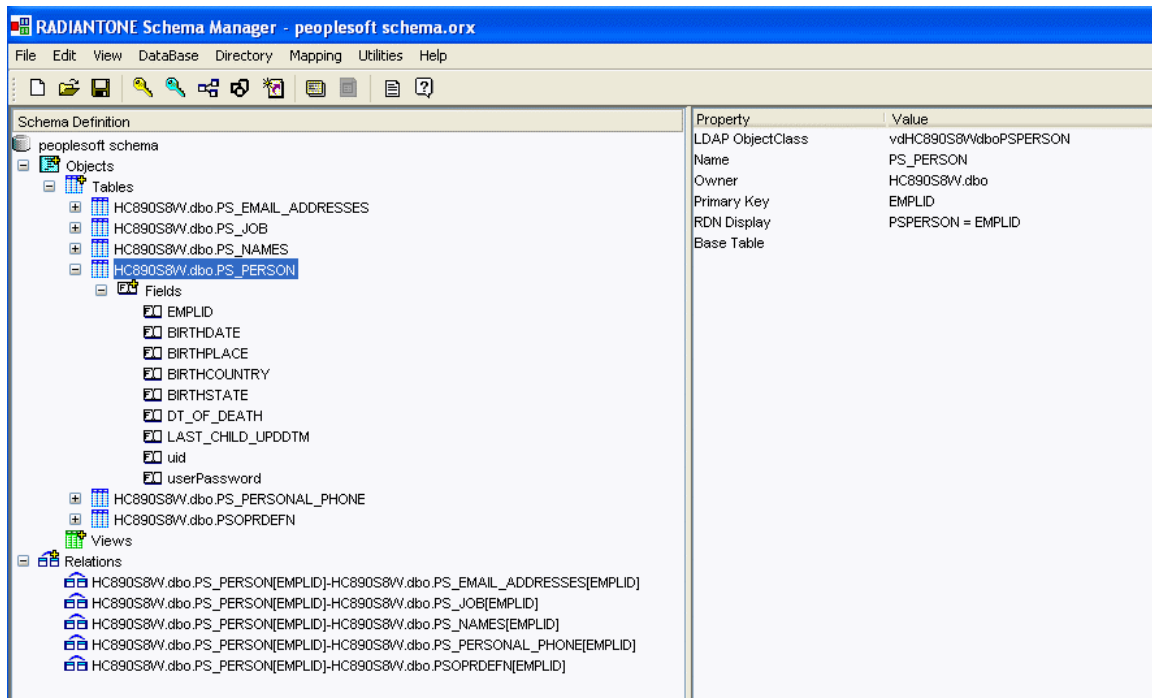


Figure 3 – PeopleSoft HRMS schema and defined primary key and relationships

With the schema extracted and enhanced through the declaration of primary keys & relationships undefined in the PeopleSoft HRMS source, the next step was to translate this relational schema to a hierarchical LDAP-based view using the Directory View Designer.

Virtual view modeling and design. Two virtual views were created from the refined schema. The context for the first view (PSOFTHRODBC) was basic employee information. This view was also configured as the view for authentication and authorization. The context for the second view (PSOFTLOOKUP) was PeopleSoft user information. The following table lists the two views and the attributes they contained, with mappings to the PeopleSoft HRMS schema:

Radiant Logic View Name	View Attribute	PeopleSoft HRMS TABLENAME.ATTRIBUTE
PSOFTHRVIEW	EMPLID	PS_PERSON.EMPLID
	EMAILADDR	PS_EMAIL_ADDRESSES.EMAIL_ADDR
	JOBCODE	PS_JOB.JOBCODE
	PHONE	PS_PERSONAL_PHONE.PHONE
	PHONETYPE	PS_PERSONAL_PHONE.PHONE_TYPE
	EADDRTYPE	PS_EMAIL_ADDRESSES.E_ADDR_TYPE
PSOFTLOOKUP	OPRID	PSOPRDEFN.OPRID
	EMAILID	PSOPRDEFN.EMAILID



An interception script was created to correlate employee information with PeopleSoft user information, for the purpose of defining a unique identifier for the virtual view. The script performs a lookup to see if a specific EMPLID has a corresponding OPRID value. If it does, then the OPRID value will be used to populate the *uid* attribute (the unique identifier for the virtual view). If no value for OPRID is found, then the first part of the employee's email address is used to populate the *uid* attribute.

LDAP Authentication and authorization delegation. Using the existing PeopleSoft Financials application LDAP client (with no modifications), a user logged into the Radiant Logic virtual LDAP server. The security token and credentials were accepted by the Radiant Logic virtual LDAP server, and passed back to the PeopleSoft HRMS application, which did the actual authentication and authorization. To the PeopleSoft Financial application user, it appeared as if the virtual LDAP server performed the authentication and authorization. Now logged in, the PeopleSoft Financials user could make requests for HRMS data.

Lookup. The PeopleSoft Financial application user requested a lookup of the virtual HRMS view. One possible scenario is verifying employee identity and email address prior to sending out an expense report. The request was bound to the virtual server, which invoked the custom interception script defined during the virtual view design process. The result was then delivered to the PeopleSoft Financial application, completing the transaction. The following diagram illustrates the lookup process, using the interception script:

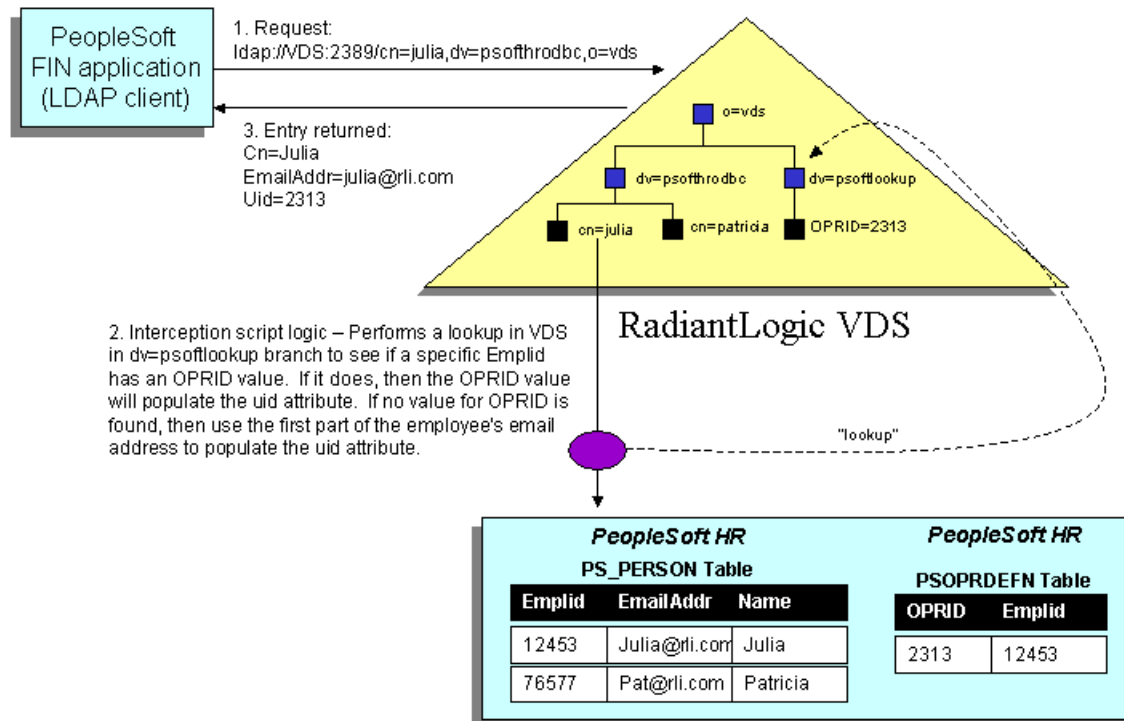


Figure 4 – Interception Script Logic for lookup

The Proof of Concept demonstrated several important capabilities of a PeopleSoft-Radiant Logic integrated identity solution:

- **Security** – a more robust, extensible LDAP layer that can provide transparent delegation when needed
- **Availability** – virtualization of source data in real-time obviates the need for costly data replication
- **Flexibility** - context-based virtual views allow new attributes and joins, without changes to source data; interception scripts handle special situations

These capabilities map perfectly to the management challenges presented in the Introduction of this paper. The last two challenges, cost containment and growth, are addressed inherently in the solution's capabilities. In terms of cost containment, the nature of dynamic access gives an immediate cost avoidance benefit for application development and maintenance, since no modifications are necessary to applications or underlying data to change the views. And the combination of flexible features, open standard support, and scalable architecture, means that businesses employing



the PeopleSoft-Radiant Logic combination as their authoritative identity management and provisioning system today, will be well-positioned for future growth.

Conclusion

This paper has presented the case for PeopleSoft HRMS as an authoritative source of identity information in the enterprise, realized in evolutionary steps. These steps can be summarized as follows:

1. **Establish the Authoritative Source.** PeopleSoft HRMS is the starting point for identity data in the enterprise, so is the natural authoritative source. However, PeopleSoft did not speak the same language as most identity-oriented applications, limiting the ability to leverage PeopleSoft HRMS as the authoritative source.
2. **Standardize the interface.** PeopleSoft's LDAP interface made it much easier for identity-oriented applications to access PeopleSoft data. Consequently, the increased access and usage brings several management challenges.
3. **Virtualize.** The addition of Radiant Logic's virtual directory solution enables PeopleSoft HRMS to meet the challenges posed by increasing usage.
4. **Evolve.** The PeopleSoft-Radiant Logic combination grows with businesses as they evolve and update their identity management and provisioning infrastructure.

The combination of PeopleSoft HRMS and Radiant Logic provides a quickly deployable and extensible infrastructure for businesses that want to fully leverage PeopleSoft HRMS today as the authoritative source for identity, while positioning themselves for future growth.

For more information:
415.209.6800 x150
info@radiantlogic.com