Sharing Department of Labor's SOA Infrastructure - Architecture

Prepared by

Enterprise Planning and Architecture Strategies Team

Control Page:

Revision History:			
Version No	**Revised Date**	**Author**	**Comments**
	07/14/2011	Anitha Ramakrishnan	Initial Version

Table of Contents:

1 Introduction:

The New York State Department of Labor has adopted Service Oriented Architecture (SOA) to modernize and automate business processes. In order to support SOA's loosely coupled architecture, Service Level Agreements and end-to-end security requirements, a secure, resilient and flexible SOA Infrastructure has been built.

1.1 Purpose:

The purpose of the document is to outline the Department of Labor's Infrastructure architecture and the potential to share infrastructure services with other NY State agencies to host their applications / services.

This document is intended for Business Managers, IT Managers, Enterprise Architects, Application Architects, Technical Leads and Developers.

2 Department of Labor's Infrastructure Architecture:

Our enterprise architecture is based on SOA with process centric programming model (BPM), using an Enterprise Service Bus (ESB) for integration and Business Process Execution language (BPEL) for process orchestration. The BPM-SOA combination allows services to be used as reusable components throughout the enterprise that can be orchestrated to support the needs of business processes.

As with software, infrastructure is also a service in SOA. It provides the foundation for IT services. Major infrastructure services include security / access (authentication and authorization) services, service level management (SLM) services and monitoring services that are shared across the enterprise and are used to optimize throughput, availability and performance.

The major components in our infrastructure are

1) Web Services / Security Gateway:

WebSphere DataPower is used as our web services/security gateway.

SOA security approach

- **Security as a service:** Security service is central and not part of any application and could evolve in-line with business needs. It offers applications the ability to authenticate, authorize, encrypt/decrypt messages, sign/verify signatures and log messages.
- **Message Level Security**: Different parts of a message can be protected differently, to make them usable only by intended parties in the message path.

- **Policy-driven Security**: Security requirements must not be hard-wired into applications or services themselves. Instead security requirements should be separated from business logic and declared as policies. Policies could be business, architectural, operational.

Web services gateway

- Provides integrated message-level security (supports WS-Security, WS-Policy, WS-SecurityPolicy, WS-ReliableMessaging, WS-SecureConversation, WS-Trust, SAML, and LDAP)
- Provides protection against XML vulnerabilities by acting as an XML proxy and performing XML well-formedness checks, buffer overrun checks, XML schema validation, XML filtering, and XDoS protection.
- Provides centralized security functions and acts as an enterprise wide single security-enforcement point for XML and Web services transactions
- Integrates with WSRR and other policy decision points such as LDAP and Siteminder Policy server.
- Offers robust service level management, policy management, and Web services management support.

The gateway supports security for not just web services, but for other channels such as File Transfer Protocol (FTP), and Web applications. The Department of Labor uses NYSDS provided SiteMinder and Sun one LDAP for Authentication.

2) Enterprise Service Bus:

The Department of Labor's ESB is a ***hybrid ESB*** built on an ***ESB Gateway Pattern.*** The gateway (router) provides dynamic routing capabilities. It provides the capability to mediate, route and transport service requests from the service consumer to the correct service provider. In other words, it decouples the service consumer and providers. This provides the capability for service consumers to locate service providers and initiate service invocations securely.

The ESB is also used to expose/integrate COTS services. Additionally, the ESB provides other features like logging, synchronous and asynchronous invocation of services, protocol mediation, reliable delivery and transaction management.

3) Service Repository:

The service repository stores the contract (WSDL/XSD) and other policies (WS-policy) to support SLM that will be enforced by the gateway/ESB. We use Websphere Registry and Repository (WSRR) as our service repository and service governance tool. The service endpoints stored on WSRR are looked up by the ESB to dynamically route service requests.

4) Business Process:

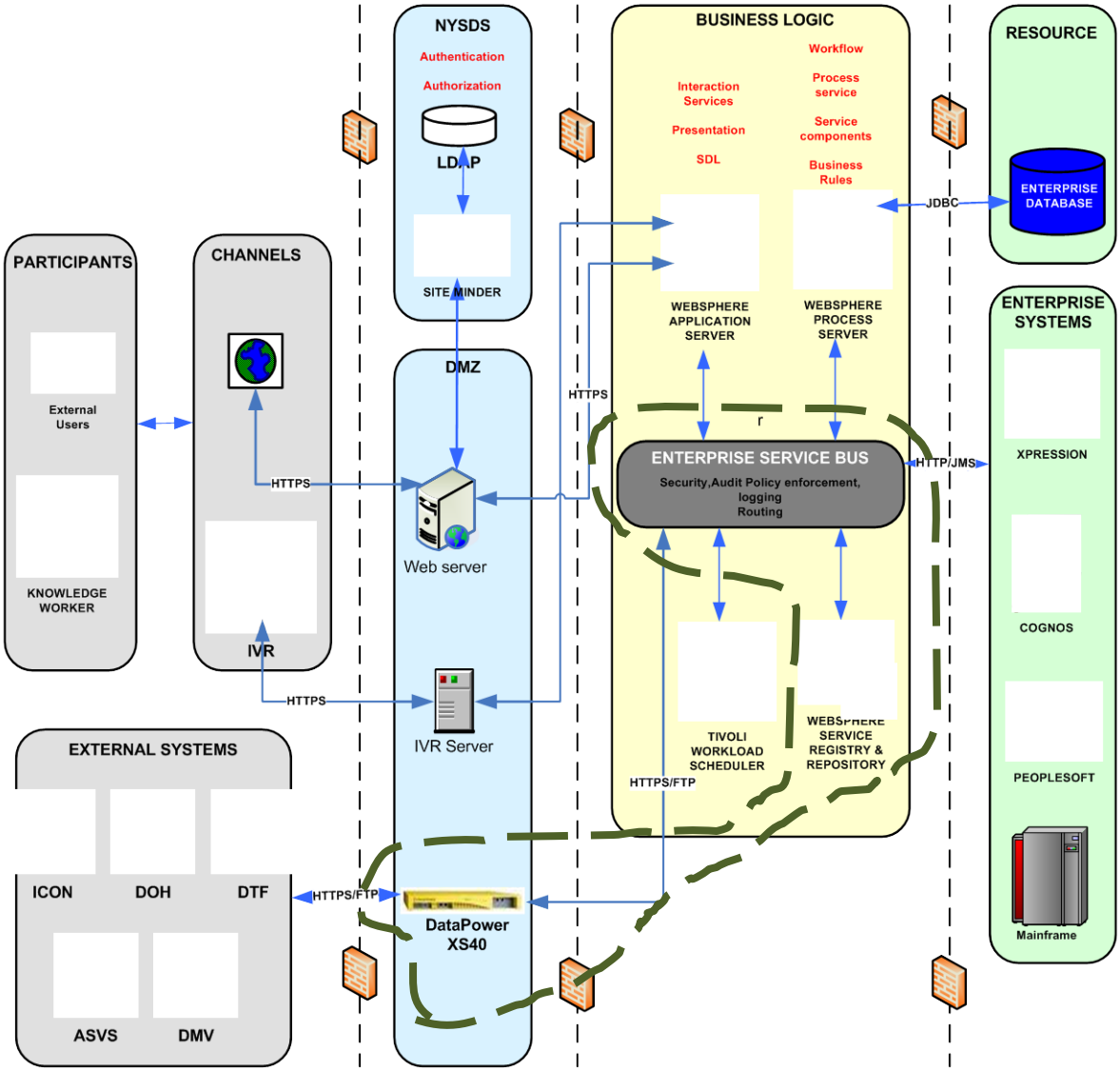
Websphere Process Server (WPS) is used to compose and choreograph services and Ilog Jrules for Business rules.

5) Enterprise/Operational Systems:

The enterprise systems/resources include the Mainframe, Oracle and other third party off the shelf products used for reporting and correspondence.

3 Potential to Share our Infrastructure - Architecture:

Conceptual Operation Model



Although all of the components in the business logic layer in the above diagram could be used to host services for other agencies, the ESB along with the service gateway (DataPower) and WSRR have the highest and most immediate potential for sharing.

Sharing DataPower (Service gateway)

The service gateway could be shared with other NYS agencies to provide security services to secure business services that they expose. This would require creating a separate domain in DataPower for the agency and implementing their security policies and requirements. The firewall rules/connectivity to connect to tier2 of the agency (where the service is deployed) will be required as well. This will help the agencies to externalize their security implementation from their service implementation and to provide a proxy to the service consumer.

Sharing the ESB

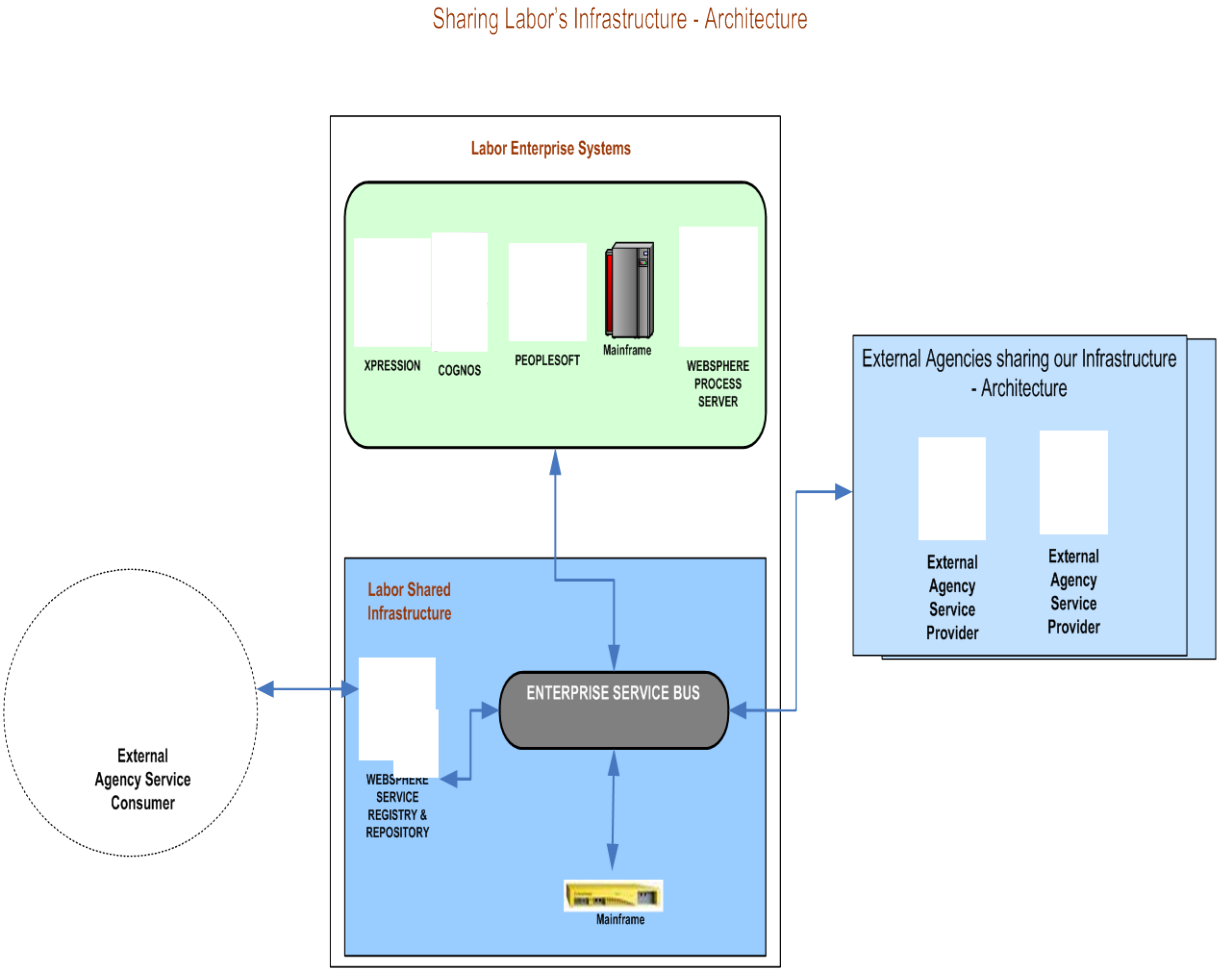
The ESB could be shared with other NYS agencies to provide the dynamic routing, mediation and transformation needs of the agency. A separate instance of the router (mediation) could be run for each agency.

Sharing WSRR

Similarly, WSRR could be shared with other agencies to host their service definition by creating a separate perspective and profile that could have a completely different look and feel and security/access based on the agency's need.

The Department of Labor's ESB and the gateway pattern can be expanded for use across State agencies. The security, routing, transformation and SLM services for other agencies could be hosted here. We also monitor these components using ITCAM.

The following diagram depicts the potential future model of infrastructure.



4 Foundational Services:

Apart from the infrastructure, we also have developed foundational services to support SOA based development and execution. These services have standard interfaces and could be shared and exposed to other agencies as well.

The foundational services provide a reusable abstraction of some of the common technical functions that could be used / extended to build SOA based composite applications. They establish standards, patterns, base components and utilities that accelerate the development of business specific implementations. The major advantages of the foundational services include:

- Increased consistency and reusability across all applications that arebuilt for Unemployment Insurance and other programs.
- Enables development team to focus on business logic rather than the complexities of implementation.
- Provide abstraction from products and technologies used in SOA implementation.

Some of the foundational services are

1. Logging Service
2. Authorization Service
3. Caching Service

5 Contact NYSDOL to share our Infrastructure Services:

Any parties interested in collaborating with the NYSDOL by sharing our SOA infrastructure, please contact us at this email address: NYSDOLServiceAdmin@labor.ny.gov.