University of California Office of the President

PPS Web Services Governance

Framework, processes, and procedures for managing the PPS web service architecture

UCOP Information Resources & Communications | Payroll Personnel Services
10/6/2010

Table of Contents

1.0 Background

1.1 What are PPS web services?

A PPS web service is a component of the distributed mainframe payroll system that allows for a real-time interactive interface between a campus/location instance of the Payroll/Personnel System (PPS) and a web application that is capable of transmitting XML-encoded SOAP messages via HTTPS protocols.

PPS web services provide the ability to re-use existing PPS business logic and software components that are currently in use as well as to develop new services to fulfill new business requirements.

1.2 Web service governance considerations

Because web services are designed for interoperability to be consumed by a variety of web applications, the PPS service architecture presents some unique governance issues which will impact business and information technology management.

- **Decision Authority**
  Effective governance of disparate PPS services and applications will require a governing body with clear decision-making authority. This body will need to incorporate business owners, technical experts, and other stakeholders from across the UC system.
- **Portfolio Management**
  Web services require more formal IT portfolio management which would elevate prioritization and oversight responsibilities to the executive level, communicate priorities, achieve efficient and effective allocation of resources, and forge a link between project selection and business strategy.
- **Budget and Funding**
  Implementation and support of web services will have an impact on IT budgets at UCOP and at the campus level, and may require a new model for estimating resource costs and charging for usage.
- **Development and Deployment**
  Web service/application development projects will be collaborative and focused on interoperability between payroll services and diverse campus applications. Deployment will involve business and technical teams from multiple locations, working in a collaborative environment to design, develop and test new PPS services. This type of inter-campus development effort requires more structured project management and communication to ensure that services and applications are built according to agreed upon architectural and security standards.

- **Operational support**
  Operational support becomes much more complex in a distributed service environment where the service resides in one environment (for instance on the UCOP mainframe) and the applications consuming the service reside on various application servers at the campus level. The governing body and IT service provider must clearly define the roles and responsibilities for troubleshooting problems and expectations for service level agreements, and disparate IT divisions must collaborate on problem resolution.

This document seeks to highlight these governance issues as they relate to the PPS web service architecture, to put these issues within the context of the larger PPS/payroll governance framework, and to offer guidelines and processes for governing web service development, usage, and support.

2.0 Web Services & Payroll Governance

PPS Web Service governance falls under the purview of the larger PPS Governance structure. It is assumed that the governing body charged with decision-making authority and responsibilities for the Payroll/Personnel System (PPS) and payroll business processing will also be charged with IT governance responsibilities related to PPS web services. Specifically, these governance roles and responsibilities with respect to web services are delineated below.

The PPS Governance structure assumes a single intake point for all requests related to payroll changes, initiatives, or information requests. This includes any requests related to development or consumption of web services.

The IT governance structure will also include a Technical Architecture Group (TAG) which will report to the management committee of the PPS Governance body. The Technical Architecture Group will be comprised of programmers, architects and technical experts from across the UC system, and will be responsible for providing application developers with specific and actionable feedback on design specifications as needed. The Technical Architecture Group will be vested with the authority to approve or deny design specifications if the technical implementation will have an adverse impact on system security, application performance, or the integrity of the overall web service architecture.

2.1 Approval of Campus Request to Consume a Web Service

The new PPS web service architecture will serve as an interface both for web applications built by UCOP *and* for web applications built by campus departments and medical centers in response to local business

needs. Examples of this business case in which a campus or medical center wishes to integrate with or "consume" a PPS web service include:

- A location developing a web-based time and attendance application to interact with the PPS time reporting service
- A location developing a web-based expense transfer application to interact with a PPS expense transfer service
- Campuses or medical centers implementing PeopleSoft HCM to interface with the location PPS via EDB entry/update services

The PPS governing body will evaluate a web service consumer request to gauge whether the requestor has authority to build an application interface to the payroll system, and to evaluate whether the request is similar to another initiative and thus recommend a coordinated, collaborative effort among multiple project initiators. For example, efforts undertaken by multiple medical centers to implement an HRIS system present an opportunity for cross-campus collaboration with an eye toward consistency and common business practices.

The Technical Architecture Group will also review requests to consume a PPS web service, with the objective of ensuring that the consuming web application adheres to the established standards for IT security, performance, and architectural integrity.

See "*PPS Web Service Requests – process flow*" for more information.

2.2 Approval to Add a New Web Service to PPS

As part of UC's continued efforts to implement a full-featured web-based interface for the payroll system, many new web services might be developed and deployed to support new browser-based user functions. The PPS governance body will be responsible for approving and prioritizing any new development efforts. This will allow the governing body to manage the overall PPS development portfolio and to administer the suite of web services offered to campuses.

If the PPS governance body wishes to pursue a full Service-Oriented Architecture (SOA) in the future, then a more robust governance structure may be established to support campus development of web services. Until that time, it is envisioned that UCOP will design, develop, and deploy PPS web services centrally.

2.3 Approval to Modify an Existing PPS Web Service

PPS web services are designed to be as generic and interoperable as possible, to support usage by web applications developed by UCOP IR&C and by campus application developers. Because the services will be used by multiple consumers system-wide, it is imperative that modifications made to the services are tightly controlled and communicated to all registered web service consumers. In order to ensure general

stability of the web services, modifications will be deployed as infrequently as possible and be limited to critical error fixes and high priority enhancements.

The PPS governing body will have the authority to approve and prioritize any modifications to existing PPS web services. The Technical Advisory Group will review any requested change to an existing service to determine whether the modification should be made to the base service or whether the change may be implemented as a local version of the service program. It is noted that any approved local modifications will be strictly limited to COBOL program components. The WSDL interface of any service shall remain unchanged.

For any approved modifications, the governing body and the service provider will communicate the changes to all registered web service consumers so that campuses may coordinate corresponding changes to local web applications. In addition, UCOP IR&C, as the web service provider for campus payrolls hosted at UCOP, will be required to coordinate testing and deployment with all registered web service consumers.

2.4 Audit Oversight

The Payroll Governance body, working in conjunction with the Technical Architecture Group, will be responsible for audit oversight of web service consumers to ensure compliance with established security protocols outlined in this document. The frequency and nature of the auditing process will be the prerogative of the payroll steering committee. However it is executed, the audit should result in reports which detail recommendations and findings where non-compliance is identified. Non-compliance with established security policies and procedures will result in the campus web service SLA being terminated.

3.0 IT Governance and Application Development

3.1 Design and Development Guidelines

All web applications that interface to PPS via PPS web services shall adhere to defined architectural guidelines and programming standards. As part of the governance process, web application developers must submit their application design specifications to a Technical Advisory Group for review.

See companion document "Application Development Standards and Guidelines" for more information.

3.2 Application Documentation

Application developers deploying web applications that consume PPS web services will provide application documentation to the IT service provider (UCOP IR&C for campus payrolls hosted at UCOP). Application documentation must be sufficiently detailed to support performance monitoring, troubleshooting, and problem resolution for the web application and/or web service.

Documentation will include the following:

- Application data and process flowchart, including web servers, application servers, load balancers, etc.
- Anticipated application transaction volume per anticipated cycle (i.e. number of transactions anticipated, anticipated high usage times (daily, monthly, quarterly, annually, etc.)
- Other system documentation deemed necessary to support the service interface

3.3 Security Requirements

Web Services have special security requirements because, if left unsecured, they could be accessed from any server attached to the World Wide Web. Three mechanisms are used to provide security for PPS Web Services.

SSL encryption of all data sent or received via TCPIP

PPS Web Services will reject any request that is not encrypted via SSL and using SSL encryption on outgoing messages.

Authentication and Authorization of Web Servers[1]

Only authenticated University of California web servers can access PPS Web Services. Server authentication is done by requiring the requesting server to present a client certificate as part of the SSL handshake. Requests for service are not honored unless the client certificate presented to the hosting CICS region is associated with a RACF id on our z/OS system[2].

Once authenticated, only authorized web servers are allowed access to a PPS Web Service. Authorization is based on the RACF userid assigned to the client certificate issued to the web server.

Authorization to use PPS Web Services in any given CICS region is controlled by CICS transaction security applied to the CICS transaction id under which all web services start execution.

End User Logon

All PPS Web Services that access sensitive data also require a valid token as part of the request. A valid token can only be obtained in response to a successful logon made via the PPS Logon Web Service. As a result, the logged on end user's RACF id is available to PPS Web Services. The application level authorizations that are part of PPS CICS EDB Entry/Update are enforced by PPS Web services base on the end user's id.

If a security breach occurs, the service consumer location should initiate standard breach procedures and notify the service provider of the incident.

4.0 Operational Support Procedures

4.1 Procedures for Campus Consumption of PPS Web Services

Once the PPS governing body has approved a campus request to consume an existing PPS web service, UCOP Information Resources & Communications, the service provider for campus payrolls hosted at UCOP, will coordinate with the campus requestor to define the implementation timeline, testing needs, and application development requirements for the campus web application.

In order to consume a PPS web service, the requestor must certify that the campus entity will provide the appropriate level of operational resources to support and maintain the campus or medical center web application. In the event that the local application is no longer supported, the location must contact the service provider immediately to terminate the Service Level Agreement.

[1] Point to point security is implemented using HTTPS to perform both client and server authentication. No intermediary access to the encrypted message is possible (e.g. proxy server). Note that authentication is technically performed against the application server.

[2] The mainframe systems group at UCOP has established a Certificate Authority to issue certificates and assign a RACF id to each one.

To initiate the process, the campus should submit a completed Web Service Integration Request Form containing all relevant data related to the request.

The process for developing and deploying a web service-enabled campus application will be comprised of the following steps:

Step	Owner	Action
1	Project Sponsor	Complete request for PPS Web Service Integration, including signed Trust Agreement and Certificate Request form
2	PPS Governance Body	Review request. Approve or deny request, or return to project sponsor for additional information.
3	PPS Governance Body – Technical Architecture Group (TAG)	If the request is approved, the TAG reviews request TAG sends architectural and security guidelines to project sponsor, and routes request to service provider
4	Service Provider (IR&C for all campus payrolls hosted at UCOP)	Service Provider assigns resources for consultation and implementation Service Provider coordinates with the infrastructure support teams (mainframe systems, network, monitoring, operations) to discuss operational considerations Service Provider meets with project sponsor to discuss timeline, testing requirements, and certificate requirements Service Provider establishes test environment for sponsor
5	Project Sponsor	Develop design documents for web application Submit design documents to Technical Advisory Group for review Submit request for digital certificates (if this form was not included in initial packet)
6	PPS Governance Body – Technical Advisory Group	Review design for adherence to architecture and security standards. Provide feedback to Project Sponsor.
7	Project Sponsor	Revise Design based on TAG feedback Develop and unit test application Perform integration testing
8	Service Provider	Provide support for vulnerability and stress tests
9	Project Sponsor	Execute vulnerability and stress tests on the web application
10	Technical Advisory Group	Review results of vulnerability and stress tests
11	Project Sponsor	Review and approve Web Service SLA Implement web application in production
12	Service Provider	Administer Service Level Agreement

4.2 Certificate Authority Procedures, Roles & Responsibilities

For PPS web services that are part of a campus payroll instance residing on the UCOP mainframe (all hosted PPS locations and UCSF), UCOP IR&C is the sole Certificate Authority (CA) with authorization to issue digital certificates. The University of California Los Angeles is responsible for issuing its own digital certificates for web service consumption where the service provider is the UCLA payroll instance.

It is noted that the Governing Body may choose to set a maximum number of certificates that may be issued to a campus or location, in order to control operational costs and manage risk. The Service Provider must conform to this maximum, if the Governing Body chooses to enforce it.

Web Service Trust Agreement

As part of the process to receive a digital certificate necessary to consume PPS web services hosted at UCOP, the campus Chief Information Officer (CIO) or Campus Security Officer must submit a signed Trust Agreement governing access to hosted web services. Production certificates will not be issued until a signed Trust Agreement has been received. By signing this document the campus is certifying that they will conform to the following policies and requirements:

1. Certificates issued to allow access to a UCOP hosted Web Service must only be used by the application that applied for it. A certificate may not be moved or copied for use by another application.

2. Certificates issued to allow access to a UCOP hosted Web Service must only be used for their intended purpose, i.e. access to the production, quality assurance, or test web service.

3. All processes run using certificates that have been granted production access must be run using audited controls. Processes that run without audited controls (i.e testing, QA, etc.) must use a certificate issued for that purpose. A certificate may not be moved or copied for use in another environment other than the one for which it was issued.

4. Applications that use a UCOP hosted Web Service must be audited for compliance with these policies by their campus Security Officer at the time a certificate is issued to allow access to the Web Service and annually when the certificate is re-issued.

Certificate Request Form

In addition to the Trust Agreement form submitted by the CIO or campus Security Officer, the requesting location must submit a Certificate Request Form to receive a digital certificate for development, test (QA), and production environments. Digital certificates are valid one year from the date of issuance. The Service Provider will notice the customer as expiration dates approach; however, it is the campus' responsibility to renew the certificate prior to expiration.

For each digital certificate issued, the Service Provider will document the following information:

- Certificate Label
- Certificate Begin Date
- Certificate End Date
- Associated RACF ID
- SDLC status of the application using the certificate (development, test/QA, production)
- Application Server name on which the application resides
- Dot decimal URL of Application Server name on which the application resides
- URL used to access the application
- Customer contact information

4.3 Service Level Agreements for UCOP Hosted Applications

For payroll locations hosted at UCOP, implementation and support of PPS web services requires addendums to existing Service Level Agreements (SLA). There are two types of addendums available depending upon the type of web service and/or web application being supported:

1. **PPS Web Application Service Level Agreement**
   This Service Level Agreement explains availability, service level expectations, and troubleshooting guidelines for campuses which choose to install *PPS Web EDB Update* applications and other web-service enabled Java-based web applications built and deployed by UCOP IR&C, including *Web EDB Inquiry, Web PAN*, and *Web Merit*.

2. **PPS Web Service SLA**
   This Service Level Agreement explains availability, service level expectations, and troubleshooting guidelines for campuses which deploy web-service enabled applications built at the local level to consume PPS web services.

4.4 Testing Support

When a location has received approval from the governing body to build a local application which will consume PPS web services, the Service Provider (IR&C for all UCOP hosted campuses) will coordinate with the campus to identify testing needs and support.

The Service Provider will provide the location with a cost estimate for testing support, which may include establishing an appropriate CICS test environment, campus data load, and analytical support during testing phases.

Prior to production implementation, the location that has developed the web application to consume PPS web services is responsible for performing a security vulnerability scan and a load/stress test. Results from these tests will be reviewed by the Governing Body Technical Architecture Group to ensure adherence to security and performance standards.

If the campus does not possess tools or services to conduct the necessary vulnerability and stress tests, the campus may engage the Service Provider to provide these testing services on a recharge basis.

4.5 Web Service Registry

The IT Service Provider will maintain and administer a registry and repository for all web services in operation. The Service Registry will contain information about services, such as the service definitions, interfaces, operations and parameters, while the Service Repository will be used to store metadata related to the governance of service usage. A web service registry and metadata repository provides the following core capabilities:

1. Publication of available services
2. Locating the services available to a service consumer
3. Enhancing performance through management of service performance data and metrics
4. Management of information across the enterprise
5. Governance of services throughout the service life cycle

It is assumed that appropriate tools and processes will be in place to govern web service registry and metadata storage.