



LaGov ERP Project

Business Blueprint



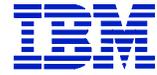
Table of Contents – Section #3

D. Portal and Security Definitions.....	1218
1. Portal Definition	1218
2. Security Definition.....	1222



LaGov ERP Project

Business Blueprint



D. Portal and Security Definitions

1. Portal Definition

Executive Summary

This document outlines the future state of LaGov Enterprise portal and going-in position for the portal deployment at the State of Louisiana (LaGov).

This document will provide the reader with information on:

- Initial deployment of LaGov Enterprise portal
- Enabling various business applications on Enterprise portal
- User enablement for both LaGov employees and LaGov suppliers with single point of access to information through a Web-based interface
- Content management on Enterprise portal

The general strategy is to leverage the existing LEO Portal Infrastructure and administration. The LEO portal provides a single point of access to a variety of employee information and services. The LEO portal is for State Employees only. Here employees can access pay statement information, travel reporting, and benefit plans. It also provides a state employee directory. The essential change will be three fold.

1. Once logged in, users will be provided an option of going to any of the SAP systems (ECC, SRM, CRM, BI including BI-IP), for which they have authorization.
2. There is also an expectation that Purchasing Suppliers will be able to self-register in order to participate in the Bid and Award processes.
3. There is also the expectation that non-state agencies will be able to apply for Grants through the expanded portal.

For the most part, enabling various business applications on Enterprise portal will mostly be in the SRM, BI, and CRM areas. The portal deployed here will be limited to SAP systems only. The Single-Sign-On concept is limited to SAP systems. Agile users are expected to access that application directly.

To-Be Process Description

As in the current environment, all users are authenticated through HCM system. All content is deployed manually after it has gone through the proper Dev->QA-PRD promotion process.

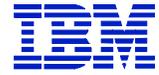
The To-Be process details the going in position for deployment of LaGov Enterprise portal integrating various Business applications that includes SAP ECC, SAP SRM, SAP BI, SAP CRM thus providing single point of access for LaGov employees and LaGov external business partners (i.e. suppliers).

For integration of various business applications on Enterprise portal, standard SAP delivered Business Packages will be leveraged along with Single Sign-On (SSO) ticket for users enabling single point of access via Enterprise portal and accessing their business transactions depending on the users' authorization settings.



LaGov ERP Project

Business Blueprint



Nomenclature Clarification: Within the IT industry, the Single Sign-on concept is sometimes an indication of single sign-on to any and all applications within an Enterprise. The use of the term Single Sign-on here refers exclusively to the passing of a user certificate from one SAP system to another. Using this technology, any links to Non-SAP applications from the portal will require a unique sign-on to that non-SAP system. The Single Sign-on (SSO) ambition here refers only to SAP systems within the LaGov enterprise. Seamless integration is only between the SAP implemented systems. Similarly, the use of the term "Enterprise" for the most part is in reference to the SAP enterprise collection of systems. In the future, systems that are determined to support SSO tickets, it might be possible to include these systems within this architecture.

SAP Enterprise Portal Deployment

LaGov Enterprise portal will be deployed with integration to LaGov website so that users, both LaGov employees and LaGov suppliers, can invoke LaGov portal directly using an URL on LaGov website.

SAP Enterprise portal is often called SAP NetWeaver Portal and runs on NetWeaver Application Server (formally known as SAP Web Application Server). NetWeaver Portal comes with Knowledge Management component, which is an integral part of Portal Server.

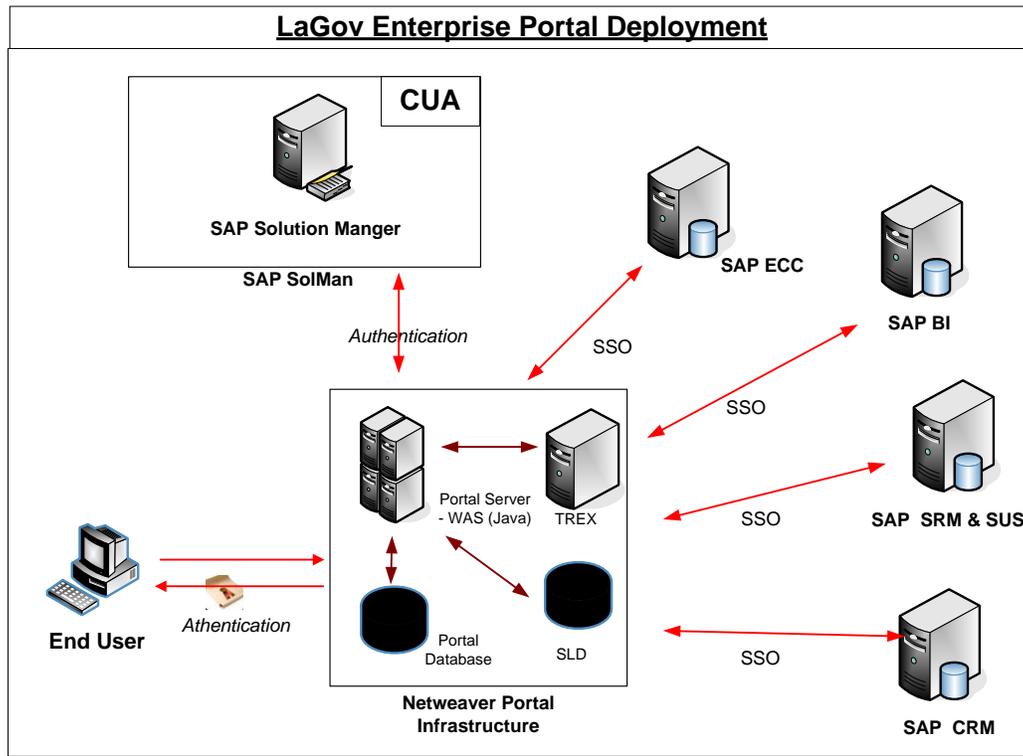
The System Landscape Directory (SLD) of SAP NetWeaver is the central directory holding the system landscape information. The SLD server stores the information about all the SAP Systems that are in landscape (SAP ECC, SAP SRM, SAP CRM, SAP BI, SAP BI-IP, etc.)

TREX is SAP Portal's Search engine that will be used for searching KM repositories objects. TREX Server is part of the portal Infrastructure but is physically installed on a separate server. TREX search is limited to Portal's unstructured KM Repository objects.

LaGov portal will be integrated with SAP ECC, SAP TREX, SAP SRM, SAP BI, SAP BI-IP and SAP Solution Manager. The integration will provide a seamless and smooth authentication to backend applications via Single Sign-On (SSO) process through SAP Logon Ticket and/ or User mapping techniques.



LaGov ERP Project Business Blueprint



- Single Sign-on (SSO) refers only to the exchange of a certificate between SAP systems
- Portal Version 2004s/Netweaver 7

User Enablement in portal (LaGov users & LaGov Suppliers)

The SAP Portal Platform utilizes the security mechanisms provided by the J2EE Engine, including user authentication, single sign-on (SSO), authorization, and secure communication. The portal depends on authentication service to implement the SSO mechanism that uses encoded cookies, to securely resolve user authorization and authentication across multiple sources of information for a user. For example, user provides the credentials on the Logon Page; the Portal server verifies the credentials according to pre-defined rules to get additional user information. When a user launches an iView, the client sends an HTTP or HTTPS request to the Portal Runtime (PRT). The PRT parses the request and identifies the requested object from the PCD. If the user that made the request has permissions for the requested object, the PRT obtains an instance of the portal component to be executed, provides it together with any other information obtained from the PCD and launches the content in the browser.

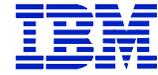
With Single Sign-On (SSO) method, LaGov portal allows the users to access various system components SAP ECC, SAP SRM etc. without having to logon to different applications to view the content. LaGov To-Be portal will be configured to enable the user access information from various applications with signing in once.

Role assignment and transaction authorizations for LaGov users will be managed centrally from within CUA (Central User Administration, called parent) system and is distributed to child systems e.g., SAP SRM, SAP BI, BI-IP, Portal etc. Portal user can access only those business transactions that they have authorization for in the respective business system. Portal authorization defines which portal content Directory (PCD) objects (Ex: folders, iViews, Pages, Roles) a user can access and which actions they can perform within the Portal.



LaGov ERP Project

Business Blueprint



For details on user management and role assignment including the 'position based security authorization control' is defined in a separate document.

Content Management

SAP Knowledge Management (KM) is an integral component of SAP NetWeaver and is delivered as part of SAP Enterprise Portal. SAP KM provides access to the information residing in the repository. Powerful retrieval & classification mechanisms and document services such as rating, feedback, and discussions allow the users to create and access information they need for their daily work.

Some of the KM services that will be configured for the LaGov Portal are:

- Viewing and editing content
- Versioning content (i.e., automatic retention of past revisions)
- Storing and retrieving content
- Deleting content

LaGov portal will utilize SAP's out-of-box features for content management. Content management is responsible for storing documents together with their content and properties, obtaining documents from various sources, and providing basic document services, such as structuring, navigation and version management. TREX is used to conduct basic and advanced search on all unstructured content and their attributes. TREX maintains indexes of CM repositories.

LaGov portal content is categorized basically into

- Unrestricted content
- Restricted content

Unrestricted content can be displayed to any user even without having a portal user account setup and is available for any user navigating to LaGov portal. Examples of such content are 'How To Guides' for Supplier Registration process, Publishing Bid Invitations for public access, Report on LaGov approved suppliers for public access, Awarded contracts for public access etc.

On other hand, restricted content on LaGov portal can be displayed only by users having Portal user account setup and hence requires login to LaGov portal. Examples of such content are Report on Payments for a given supplier and all other executable business transactions.

Typical lifecycle for content management on portal is as follows:

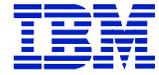
- Content is collected from business areas for delivery through the portal.
- Based on the enterprise's business area (e.g., Purchasing, Supplier Management, Grants Management, Financials, Accounts Payables etc.) and on the identified content inventory, a folder structure is designed to organize the content.
- Repository folders will be designed based on specific permissions. Once the permission for the corresponding folder is set, a content author can upload content into a folder and edit existing content in the portal.
- Content access management will be controlled by setting the folder permissions at user level or group level. KM uses the central Portal UME and its services.
- New versions are generated when there is new content created or changes made to existing content.

SAP TREX is capable of indexing unstructured data such as the contents of text-containing documents (e.g., MS Word documents) as well as capable of indexing many languages. In LaGov portal, an index is created and configured for each portal repository folder. Permissions will be set and managed in the index level and the TREX scheduler is set to run on daily base so that any new content uploaded to KM repository during the day will be indexed at the end of the same day and be available for searching afterwards.



LaGov ERP Project

Business Blueprint



To-Be Process Supported by the Portal

The following Application Component Processes will be support by Enterprise Portal

ECC

All the to-be processes that are designed to be carried out in ECC system will be executed in portal using the standard SAP delivered Business packages. These processes include both Financial & Logistics processes.

SRM

All the to-be processes that are designed to be carried out in the Supplier Relationship Management (SRM) system will be executed in portal using the standard SAP delivered Business packages. These processes include Procurement & Sourcing.

Additionally, the SRM-SUS processes that involve collaboration with suppliers, Supplier Registration and Bid submission will be enabled in portal.

CRM

The key Customer Relationship Management (CRM) processes to be supported by the Enterprise Portal include the ability for non-state agencies to be able to apply for Grants through the expanded portal.

BI

The key Business Intelligence (BI) processes to be supported by the Enterprise Portal includes posting of some reports and dashboards to the portal. For the most part, the portal will pass control the Business Objects WEBi front end for access to reports. Portal Support will also be necessary for Vendor Evaluations.

BI-IP

All end-user Budget Prep processes of Business Intelligence – Integrated Planning (BI-IP) are to be supported by the Enterprise Portal including budget data entries.

Any custom transactions that are developed within ECC / SRM calls for FRICE-W development in Enterprise portal and details for such objects will be defined during Realization.

2. Security Definition

Executive Summary

The purpose of this document is to define the procedure for managing security for the LaGov project.

This includes security organization structure, roles, responsibilities, user administration and role administration. The administration of roles requires procedures for functions creating and changing roles. The administration of users will be automated to create and delimit end users. Procedures for functions such as manually creating user master records, changing user master records, resetting passwords and monitoring security relevant user activities will be documented.

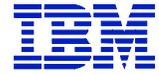
Due to the dynamic configuration environment of the LaGov, it is important to note that this process will change as business processes are defined and fine tuned and the changes are represented in LaGov. It is therefore important to document each change as it impacts the strategic direction of the project.

The scope of this document is to define the security process, procedure and associated tools for the LaGov security administration process.



LaGov ERP Project

Business Blueprint



To-Be Process Description

The approach to LaGov security is to centralize the maintenance of authorization roles and objects using Central User Administration. The organization structure within ECC will be used as the basis for a position based security strategy. The underlying assumption is that employees or users require appropriate authorizations to perform the tasks expected of their position. Each position within the organization structure will be represented by a single or composite role. If the employee associated with the position changes, we will not need to assign the security role(s) to the new employee as the roles will be inherited from the position. In this way, the new employee automatically receives the roles through the position. If an employee changes position, the personnel administrator assigns a new position to the employee. This means that the employee loses the authorizations that belonged to his or her old position, and receives the authorizations for his or her new position. Since the ECC is the only system maintaining an organization chart, derived roles will be determined in the ECC and then pushed to the child systems.

Central User Administration (CUA)

To facilitate central point of user administration, our approach going to use CUA (Central User Administration) to connect all the child systems to a central system. As today, we are going to use ECC/HCM as a central system and all other systems (BI, CRM, SRM, PI) as child systems. The exception to this is AgileAssets system which is a third party product. Connecting Agile may require a custom interface and pass security information.

Position Based Security

The approach is to use position based security across all the systems. Positions will be based on the HCM Organization Structure found in ECC. This leverages the as-is processes where the State of LA already uses the live HCM system for this purpose.

Roles and Responsibilities

LaGov security administration requires active involvement across the project team. This section defines the required roles and responsibilities.

LaGov Security team

The LaGov security team is responsible for the following activities:

- Assisting with problem resolution
- Obtaining senior management assistance to resolve complex situations.
- Working with the module/role owners and functional teams in defining and documenting the role structure.
- Design, develop, test and implement roles in LaGov based upon approved documentation.



LaGov ERP Project

Business Blueprint



LaGov Functional team

The functional teams are a member of the LaGov project team with authority and responsibility for a specific functional area (Financials, Logistics, Linear Assets, Business Intelligence, etc.). The user in this role is responsible for specifying security requirements from a LaGov perspective. Responsibilities include:

- Assessing need for specific security.
- Defining security requirements.
- Defining the content of security as it relates to roles.
- Authorizing role assignment to jobs to task within an organization.
- Requesting resources required for implementing the security solution.
- Testing the implementation of the security architecture.
- Assisting the BPO or Data Owner in identifying security conflicts.
- Testing functionality of new LaGov releases.
- Assist in troubleshooting security issues.

OCM Team

The OCM team will work with the LaGov functional team and end users to identify and define the requirements of their particular business processes. The OCM team will work with the security team when needed to update the role structures and design and development of roles that are identified after go-live. The OCM team will remain active thru the duration of the project implementation and in place for post go-live support. Responsibilities include:

- Identify tasks and activities the end user must perform in a given role.
- Present unique or unusual requirements of the business unit.
- Assist in identifying role responsibilities, knowledge, skill and training needs.
- Assist in aligning roles with jobs in their organization.

Portal Administrator

The portal administrator is responsible for creating the Portal roles and linking the Portal role to the ECC role. The portal administrator and the LaGov security administrator will need to work closely together to keep the ECC roles and the Portal roles in sync. When the security administrator creates a new ECC role, she/he will have to relay this information to the Portal administrator so he/she can link the roles accordingly.

The User Management Engine (UME) will point to backend ECC system in case LaGov will decide not to go with LDAP for authentication.

End Users

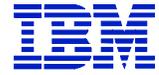
The end User is the day-to-day user of the LaGov computing resources and is responsible for protecting LaGov information responsibilities includes:

- Follow the LaGov security guidelines.
- Use only those systems and functions for which they have been trained and granted access.
- Communicate all known or suspected breaches of security policy to the Agency Security Contact.
- Protect their password and not share their access with others.
- Protect their access rights by locking the workstation when they walk away.
- Protect the workstation by logging off the system at the end of the work day.



LaGov ERP Project

Business Blueprint



Application Systems Related to Enterprise Security

The following Application Component Processes where Security will play a role:

ECC system

ECC system is HR/Financial system going act as CENTRAL system for CUA where we can control security centrally. We are going to implement position based security in this system.

BI System

BI system is reporting based system and has no HR org structure. This is going to be connected to central system using RFC. This will be treated as CHILD system.

CRM system

CRM system has no HR org structure. This is going to be connected to central system using RFC. This will be treated as CHILD system.

SRM system

SRM system has no HR org structure. This is going to be connected to central system using RFC. This will be treated as CHILD system.

PI System

PI system has no HR org structure. This is going to be connected to central system using RFC. This will be treated as CHILD system.

Agile System

This is third party tool for asset management and has no HR org structure. This is going to be connected to central system via Custom Interface. This will be treated as CHILD system.