

**California Service-Oriented Architecture (SOA)
And Federated Identity Management
Vision
November 19, 2007**

Vision Key Points for ELC Adoption

It is time for an IT infrastructure in California that supports all the diverse lines of business from an *enterprise* perspective. It should be a standards-based environment that accommodates all stakeholders – different levels of government, as well as private industry partners. To build and maintain that environment over time, we will need to establish an inclusive governance model where all stakeholders can share their views and participate in creating standards.

There are two foundational components that make up this new IT infrastructure. First, an *Enterprise* Service-Oriented Architecture (SOA) infrastructure will host and manage new web services. Many of these business services will be implemented as shared web services. Second, an *Enterprise* Identity Management (IDM) system will manage all types of users in a consistent way. It will allow for various security policies to be applied as set by various security and privacy policy organizations.

These new enterprise environments must be designed as mission critical since they will be hosting shared services supporting mission critical systems with very high availability, scalability and performance requirements.

Here are the key points of the California SOA and Identity Management environment:

Business Policies

1. Consistent with Federal standards and guidelines.
2. Designed to accommodate all stakeholders; it will support information sharing across government entities as well as public and private, subject to data sharing policies.
3. Users will be managed in a consistent way, and authentication will be at the level specified by the services they are accessing.
4. Extensive auditing capability of both user access details as well as the data they accessed.
5. All users will be managed by a number of federated “identity providers” using standard identity protocols and interfaces.
For example, “citizens” will be authenticated via a single identity service. All business service providers will “trust” this identity provider and not re-authenticate the user when accessing their services. State and local entities, as well as business partners could all be an identity provider for a certain class of users.
6. Both “local” (departments) and “enterprise” environments are supported.

That is, a department may choose to have its own SOA environment for use within the department. However, most shared services should be deployed to and managed by the enterprise environment running at DTS, Hawkins, and other major data centers.

7. If all attributes for a given class of user are not located in one repository, then a *virtual directory service* will be used to provide a single or master view.
8. If a given user will have multiple accounts (and therefore, different and possibly conflicting information), then an *identity resolution* service will be used to determine that it is the same user across the different sources.
9. The degree of “opt-in” for “citizens” needs to be determined.
That is, to what degree will a citizen have control over how and where their identity information is used?
10. A governing group will be created to manage shared services. The group will determine who owns each service and will develop for adoption policies for modifying, extending, combining, or retiring a shared service.

Information Technology Policies

11. Interoperability standards are defined; in most cases, communications will be via SOAP messaging, data will be formatted in XML, and services will have Web service interfaces.
12. This SOA environment is designed to handle online interactions via either voice or Web channels. Regardless of which input channel is used, the same services and interoperability processes will be invoked.
13. The preferred mechanism for formatting identity information is SAML embedded in a SOAP message. Stakeholders may use either WS*, SAML, or CardSpace to share the identity information (subject to sharing policies).
14. Both the local and enterprise environment can be comprised of products from multiple vendors as long as they adhere to the interoperability requirements (SOAP, SAML, XML, Web service interfaces, etc). They will also need to meet appropriate scalability and availability requirements.
15. The enterprise SOA environment primarily consists of: an enterprise service bus (ESB), a service registry, a module to govern web service policies, identity provider services, and operational policies and tools to manage the environment.
16. A service certification environment will need to be created for managing shared services.