State of California
California Technology Agency

Enterprise Architecture Standard

Identity and Access Management (IdAM) Suite Standard
Reference Model Type and ID No: TRM 1.5.885.001
Status: Approved
Analysis: (EA TRM)
Effective Date: 12/30/2010
Next Review Date: 12/29/2011
Approved By: Enterprise Architecture Standards Workgroup

Introduction

The purpose of the IdAM Suite Standard is to define the federated identity and access management software suites to be utilized by all departments exchanging authentication and authorization data between security domains within the California State government. The IdAM Suite Standard will enable web-based authentication and authorization interoperability functions including single sign-on (SSO), across sites that are hosted by multiple agencies.

Standardizing the exchange of security and authorization data between the agencies will assist in unifying disparate information systems and reduce costs associated with licensing and maintenance which will further the intent of Government Code 11545(b) (3) which is to minimize overlap, redundancy and cost in state operations by promoting the efficient and effective use of Information Technology (IT).

Standard Requirements

The IdAM Suite Standard authorizes the use of the IdAM suites provided by IBM, Oracle, Computer Associates (CA) Technologies, and Microsoft.

Authorities

Section 11545 of the Government Code (b) The duties of the Secretary of the California Technology Agency[1] shall include, but are not limited to, all of the following: (2) Establishing and enforcing state information technology strategic plans, policies, standards, and enterprise architecture.

[1] Effective January 1, 2011, the Office of the State Chief Information Officer (OCIO) is renamed the California Technology Agency (Technology Agency).

Implementation

The IdAM Suite Standard is to be used for all exchange of authentication and authorization data between security domains within the California State government. The implementation of these products and the framework for providing a federated domain trust service is identified in the State Identity Credential and Access Management Roadmap and Implementation Guidelines included as EA Practice TRM 1.5.885.002 in Section 158A of the Statewide Information Management Manual.

Changes and variances may be proposed using the Compliance Component Tools in Section 3.2.2 of the Enterprise Architecture Developers Guide, and by following the EA Compliance Package submittal instructions in Section 5.2. Additional detail is also included in Section 4.1 within the "Compliance Components Modification" subsection. The Enterprise Architecture Developers Guide is available in Section 58 of the SIMM.