

Identity and Access Management

Combining Expertise and COTS Technology to Provide Cost-Effective, Scalable Solutions

Daston Corporation provides leading-edge Identity and Access Management (IAM) capabilities to organizations throughout the public and private sector.

Overview

To create a cost-effective, secure and scalable identity and access management solution, Daston has integrated Oracle Waveset (previously called Sun Identity Manager) and CA SiteMinder with custom Java applications. Our expertise and consistent implementation of industry best practices combined with these best-of-breed COTS applications, which are consistently ranked in the Gartner Magic Quadrant, provide a full suite of user management tools that enable:

- User and attribute synchronization between corporate resources
- User self-registration to allow external DISA personnel to access DISA web-based applications
- DISANet Active Directory (AD) account creation (provisioning) and deletion (deprovisioning)
- Single Sign-On between DISA enterprise-level web applications
- User authentication utilizing the Department of Defense (DoD) Public Key Infrastructure (PKI)

This integrated solution is currently supporting the identity access and management requirements of DISA's 20,000 person user community.

Solution Architecture

Oracle Waveset is the primary tool used as the account provisioning engine and allows for the creation (provisioning) of user accounts. It is also used to disable (deprovision) accounts based on supervisor request or on account status (active, inactive, leave, etc.).

Data integrity across an organization's internal systems is maintained using synchronization and reconciliation processes developed by Daston.

CA's SiteMinder and custom web services are used for Access Control to critical internal resources. CA SiteMinder is used to enable Single Sign-On for web applications, while custom Web Services and a user-client registration application based on Public Key Infrastructure (PKI) X509 v3 certificates are used to provide user identity information consistent with enterprise attributes for internal application authorization. Login is controlled by use of the client PKI certificates that are verified via a custom Online Certificate Status Protocol (OCSP) responder.

Identity Management

Daston's Identity Management solution combines custom Java applications, Oracle Waveset, and a set of custom Apache AXIS-based web services to create and synchronize user accounts between enterprise-level resources, e.g., HR Systems, Intranet Services Directories, and File Servers.

As personnel enter and leave the organization, their accounts in the HR database are updated. Several custom-built java applications recognize these changes and either create or update accounts as required in the directory.

To support an automated account creation and disablement in the Active Directory (AD), Daston has developed several identity management custom workflows. The workflows include a deferred task approach to account for the latency in users AD accounts getting propagated through the various Active Directories. The deferred task delays the setup of the user's file shares in the Active Directory domain to insure the account is available on the file server.

Additional features include:

- A web service interface to support remote invocation of the account provisioning/deprovisioning.
- Oracle-recommended procedures for building and deploying the Waveset identity application using version control concepts and associated build scripts which simplify the building of the customized identity management application for server environments and support the efficient build-out of development, test and production servers.
- Processes/scripts that monitor the health of the Identity Management solution and notify application and system administrators when issues arise and monitor the availability of the custom java applications as well as the Identity Manager synchronization function.

Access Management

Daston utilizes several approaches to implement access management for our customers. For our DoD enterprise level users, our access management solution combines a local CA SiteMinder implementation, application integration with the Army's AKO SSO Infrastructure which is also based on CA SiteMinder, and a set of custom web services to facilitate application authorization.

The local CA SiteMinder implementation provides a client PKI certificate implementation that consists of a central web-server that performs the PKI authentication and a local OCSP responder to provide certificate revocation status.

The SiteMinder solution typically includes standard web agent integrations with SunONE Web Server, IIS 5.0/6.0 and Apache web servers as well as custom solutions for the Open Text Collaboration Server Java Authentication and Authorization Service (JAAS) module, the Oracle Waveset user interface, and several IBM Cognos implementations.

As part of a larger initiative within the Department of Defense to utilize enterprise services instead of local "enclave" services, Daston provides support for migrating Internal Web Applications to the Army SSO infrastructure as well as provides a web-services solution to translate the enterprise identity supplied by the Army into a local identity. The Daston developed web-service solution ensures users with active Army accounts and, therefore, authenticated via the Army SSO infrastructure, are not allowed entry into DISA applications.

For non-DoD customers needing access verification, Daston utilizes DataX technology that compares consumer input against more than 250 million records from both internal and public sources, including those for the USA Patriot Act, and Office of Foreign Asset Control, to instantly verify a consumer's identity. Our real-time verification service uses a combination of third party data sources that are updated on a continual basis and national in scope along with proprietary logic to assign a verification score.

For More Information

To learn more about Daston's Federated Search capability offerings, which are available on a variety of government contract vehicles, contact: Michael Pait, Senior Vice President of Business Development, 703.314.8287; michael.pait@daston.com.