

## 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. This white paper highlights the solution Daston has developed and continues to maintain and enhance for the Defense Information Systems Agency (DISA).

### Overview

To meet DISA's requirements, Daston integrated Oracle Waveset (previously called Sun Identity Manager) and CA SiteMinder with custom Java applications to provide a very cost-effective, secure and scalable solution to support DISA's 20,000 person user community. Prior to the development and implementation of this system, DISA relied on manual processes and disparate data sources to provide IAM functionality.

Daston's 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)

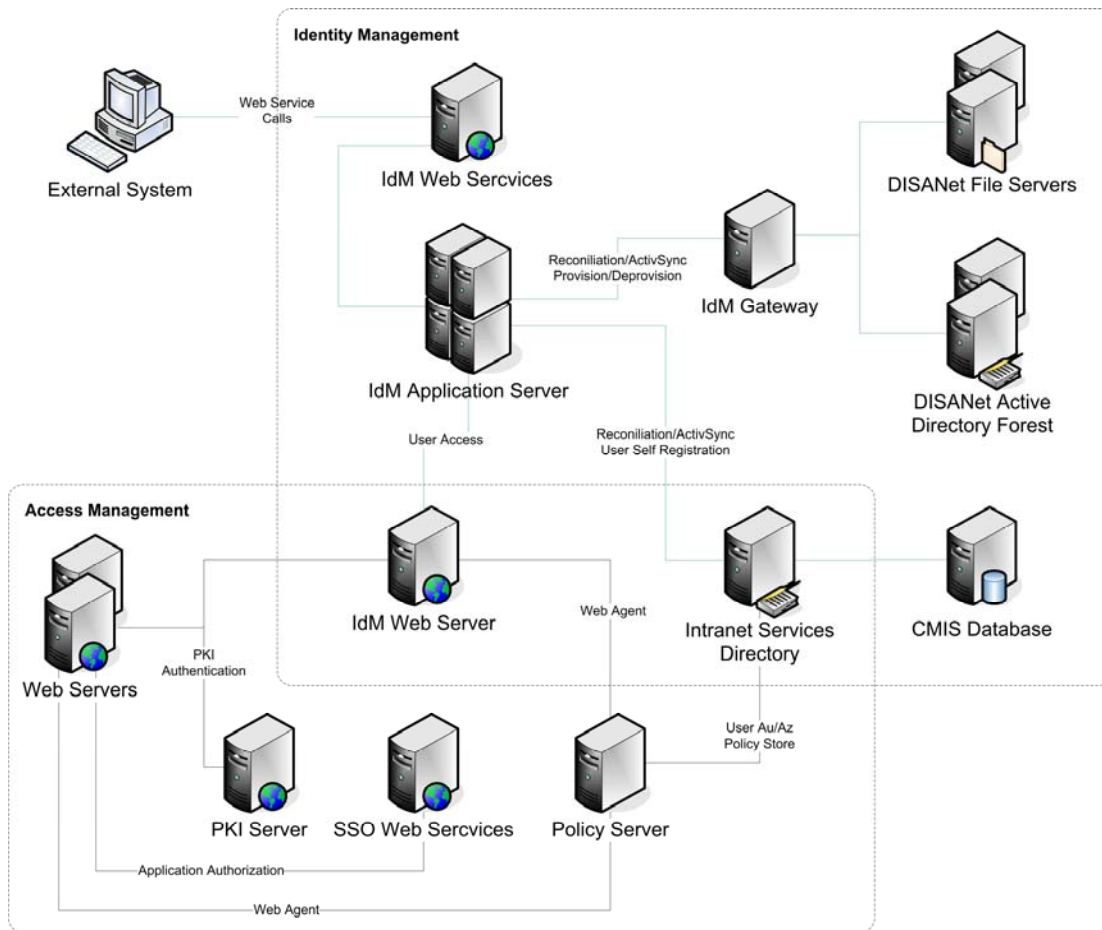
### Solution Architecture

Oracle Waveset is the primary tool used as the account provisioning engine and allows for the creation (provisioning) of user accounts within the DISA Intranet Directory Server (Sun Directory Server Enterprise Edition 5.1), the DISA Workspaces document repository (Open Text Collaboration Server), and for the DISANet Active Directory which includes all DISA Microsoft Exchange accounts.

Oracle Waveset is also used to disable (deprovision) accounts based on supervisor request or on account status (active, inactive, leave, etc.) as captured in DISA's corporate HR system which is called the Corporate Management Information System (CMIS). Data integrity across the DISA internal systems (DISA Intranet Directory, CMIS and DISANet Active Directory) is maintained using synchronization and reconciliation processes developed by Daston.

CA's SiteMinder and custom web services are used for Access Control to critical DISA resources. CA SiteMinder is used to enable Single Sign-On for DISA 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.

## Daston's IAM Solution Architecture



### Identity Management

DISA's Identity Management solution is a combination of custom Java applications, Oracle Waveset, and a set of custom Apache AXIS-based web services. The Daston solution creates and synchronizes user accounts between the following DISA enterprise-level resources:

- Manpower, Personnel, and Security Directorate (MPS) Corporate Management Information System (CMIS) - the DISA HR system
- Intranet Services Enterprise Directory (Sun Enterprise Directory Server -LDAP)
- DISANet Active Directory Forest and File Servers (Microsoft Active Directory and Exchange Server)

Custom java applications are used to create and synchronize accounts between the CMIS database and the Intranet Services Directory. As personnel

enter and leave DISA, their accounts in the CMIS database are updated. Several custom-built java applications recognize these changes and either create or update accounts as required in the directory. CMIS is considered the authoritative source for the majority of user account attributes (e.g., first name, last name, office information, etc.) and this data is synchronized from CMIS to the Intranet Directory and DISANet AD.

The DISANet AD is the authoritative source for DISA email addresses and the Intranet Directory is the authoritative source for EDIPI (PKI cert user identification number) which are synched from the Intranet Directory to the CMIS database as they are updated.

---

## Identity Management (cont.)

Oracle Waveset was chosen as the primary provisioning and deprovisioning (account creation/deletion) and user data synchronization solution for DISA. To provide account provisioning for external DISA users to gain access to the DISA Workspaces collaboration application, Daston customized the identity management system by developing a two-level approval workflow. This workflow requires users to input their information, including a Sponsor within DISA (anyone who is an active DISA user with a valid DISA email address).

Once reviewed and accepted by the Sponsor, the request is forwarded to the Approver for the Sponsor's organization. An Approver has been assigned for each DISA organization. Once approved, an account is provisioned in the Intranet Services Directory that sets the proper permissions within SiteMinder for access and creates the user account within Workspaces. All three actions are performed via customizations Daston developed for the identity management End-User interface.

To support an automated account creation and disablement in the DISANet Active Directory (AD), Daston also developed several identity management custom workflows. The workflows for account provisioning include a deferred task approach to account for the latency in users AD accounts getting propagated through the various Active Directories in the DISANet AD Forest and being available to be created on internal file servers. 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. The implementation of this deferred task concept has eliminated failed file share attempts due to account propagation latency.

A web service interface was developed to support remote invocation of the account provisioning/deprovisioning of DISANet AD accounts as well as the retrieval account status. This web service allows end users to build their own application front-ends without requiring access to the Oracle Waveset user or administrative consoles. CMIS implemented a remote invocation mechanism as part of its Supervisor On-Boarding tool for use when a new employee joins the DISA organization.

Daston also updated the DISA Configuration Management process to use an Oracle recommended procedure for building and deploying the Waveset identity application using version control concepts and associated build scripts. These procedures simplify the building of the customized identity management application for server environments at DISA and support the efficient build-out of development, test and production servers. As a result, DISA has a high-level of confidence that once an application is verified by the testing team, the same functionality can be expected in the production deployment.

Daston developed processes that monitor the health of the Identity Management solution and notify application and system administrators when issues arise. Scripts were also created to monitor the availability of the custom java applications as well as the Identity Manager synchronization function. Internal identity management functionality was customized to provide for monitoring of system level errors, the connections to identity management controlled resources (DISA Intranet Directory and DISANet AD), and the identity management repository to ensure the integrity of the deployed files for the identity management application.

---

## Access Management

DISA's Access Management solution is a combination of 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 DISA 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. By integrating with the DISA SiteMinder implementation, web applications get the benefit of Client PKI-enablement as required by the JTF/GNO without the burden of maintaining a complete PKI solution.

The SiteMinder solution 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, DISA has elected to migrate its internal portal, as well as Single Sign-On (SSO) functionality, to the Army Knowledge On-Line (AKO) infrastructure. Daston provides support for migrating Internal DISA 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 that can be used by DISA applications. 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.

## Daston Experience, Innovation and Results

Through our work at DISA, Daston has clearly demonstrated our ability to envision, create and maintain a best-of-breed Identity and Access Management solution. By coupling world-class Gartner Magic Quadrant COTS applications with our Subject Matter Experts, software developers, and industry best practices, Daston has created a customized, cost-effective production system that meets DISA's specific needs on an on-going basis and integrates seamlessly with existing infrastructure.

For more information on how we can help your organization improve and maintain your IAM system, please contact Mike Pait, Senior Vice President of Business Development, 703.314.8287.