OpenIAM Access Manager

Web Access Management made Easy

http://www.openiam.com

sales@openiam.com
# Table of Contents

- Introduction ........................................................................................................... 3
- OpenIAM Access Manager Overview ..................................................................... 4
  - Access Gateway .................................................................................................. 4
  - Authentication .................................................................................................... 5
  - Authorization ...................................................................................................... 5
    - Role Based Access Control (RBAC) ................................................................. 5
    - Fine Grained Authorization with XACML ....................................................... 6
  - Single Sign On ...................................................................................................... 7
  - Federation ............................................................................................................ 8
  - Security Token Service ....................................................................................... 8
  - SOA Security ....................................................................................................... 9
- Conclusion ................................................................................................................ 9
OpenIAM Access Manager meets the challenging demands of global enterprise systems allowing them to take control of who can access their systems and enforces corporate security policies across multiple points. It is a modern integrated platform that encompasses:

- Authentication
- Authorization
  - Role Based Access Control (RBAC)
  - Fine Grained Access Control (XACML)
- Single Sign On and Federation
- Access Gateway
- Web service Security
- Security Token Service
- Audit and Compliance

Built from the ground up using Service Oriented Architecture, it integrates seamlessly with the OpenIAM Identity Manager to provide you with the most comprehensive and flexible IAM product available.

**INTRODUCTION**

Globalization has imposed complex demands on modern security architectures. Enterprises need to control access to applications located within the enterprise as well as cloud based applications such as Google Apps, Salesforce.com and Office365. Further, organizations need to manage access for both internal and external users.

Resources may have to be accessed through a Gateway, access may need fine grained control, and applications to be accessed may be in the Cloud or depend on Saas. Federation and Single Sign on may be required for Web access management.

Faced with these challenges, enterprises have struggled to find a unified, integrated approach. Most solutions available today are either niche products, focusing on one part of the problem set or they are a suite of products that been assembled through acquisitions. Components in these suites usually have a dated architecture and integrating such a mish-mash into a single solution is a challenge in itself, often requiring an army of consultants.

OpenIAM has taken a refreshing approach to these challenges. OpenIAM designed an IAM stack, consisting of an Identity and Access Manager, from the ground up. The stack uses a unified SOA architecture where the two products share common functionality, users, policies, etc. all in a modern and highly scalable Service Oriented Architecture. Unlike other solutions, there no integration required within the stack. It supports industry standards including the ones listed below. It has matured through large deployments in various industries include Healthcare, Government, Transportation, and Telecommunications.

The rest of this document provides and overview of the functionality found in the OpenIAM Access Manager.
The OpenIAM Access Gateway extends the concept of a reverse proxy and provides a centralized approach to protect the web applications across the enterprise. The Access Gateway is a native module running within the Apache Web Server and provides the enterprise with the following benefits:

- Centralized Authentication for all web applications
- Coarse grained authorization based on RBAC
- Single Sign-On
- Integration with Federation functionality.

Access Gateway

Access Gateway Overview

- Centralized Authentication for all web applications
- Coarse grained authorization based on RBAC
- Single Sign-On
- Integration with Federation functionality.
If the access gateway is used, then all requests by the user are sent through the gateway. The gateway take care of:

- Ensuring that the user has been authenticated
- Is authorized to use the application that is being requested
- Provides SSO to that application

In addition to this, the access gateway also provides centralized session management, auditing and global logout. The access gateway also allows the organization to configure a firewall so that all direct access to application managed by the access gateway are blocked.

**AUTHENTICATION**

OpenIAM provides a comprehensive authentication solution with support for strong authentication. The following authentication options are supported:

- Password authentication
- Certificate Based Authentication
- oAuth
- OTP – RSA SecuriID

New types of authentication are being added on an on-going basis. The solution also supports “Step up Authentication” meaning that if the resource that you are trying to access needs a higher level of authentication, then the system will enforce this.

**AUTHORIZATION**

The OpenIAM Access Manager supports two type of authorization model: Role base access control and Attribute Based Access Control. Each of these models are well suited to solve business problems and are described in more detail below.

**ROLE BASED ACCESS CONTROL (RBAC)**

OpenIAM Access Manager manages Groups, Roles, Permissions and Resources. Groups are generally used to model organizational structure where as Roles are used to model a person’s function with in the enterprise. Developing an access control strategy based on Role Based Access Control provides a clean and flexible model that is easy to maintain over a long period of time. It is also model that is well suited for coarse grained authorization

In RBAC, a user (subject) is given one or more roles depending on the subject’s job. Access is determined by the subject’s role. Polices may be associated with a person’s role. For example, someone in a Bank Teller role may be permitted to access applications pertinent to his or her role, but not permitted to access applications related to someone in a Loan Officer role.
When an organization’s needs become complex, the number of roles and permissions necessary in an RBAC solution explode and an ABAC solution must be considered.

**Fine Grained Authorization with XACML**

Modern architectures, which separate infrastructure and application functions, as well as new compliance mandates for more granular access control and policy transparency demand fine grained authorization. Such a level of control is facilitated through Attribute Based Access Control (ABAC) implemented by the XACML standard.

OpenIAM’s XACML engine evaluates security policies to provide granular access control to your resources based on Attribute Based Access Control (ABAC). All aspects of access request are identified by attributes. In the XACML model, fine-grained access is controlled with policies based on Subject, Resource, Environment and Action attributes. These portable and re-usable policies are enforceable across multiple platforms.

Policies are rules that define what action, if any, a user can take on a resource. These policies may be simple or complex. Simple policies may be expressed in terms of privileges such as Read, Write, Update, or Delete. More complex policies may be used to address scenarios such as access based on geographic location or time restrictions. For example, a user’s profile may indicate that he or she is based in North America while the request may be coming from Asia. A policy can be defined to control such behavior.

In addition to XACML, OpenIAM’s design provides hooks to use a Rules engine such as Drools.
SINGLE SIGN ON

With Single Sign On (SSO) users can login once and roam unchallenged through the security realm. For end users, it reduces the burden to remember an array of passwords and reduces the need to individually login to each application. Participating applications are not required to give up their own logins and credentials. The ability to hold multiple identities, each with their own roles, permissions, access-levels and entitlements across multiple applications allows for a wide network of co-operating domains to communicate seamlessly.

OpenIAM’s SSO solution provides support for multiple protocols:

- SAML 2
- WS-Federation
- OpenID
- Proprietary applications

Since it is unlike that legacy applications within the enterprise will be SAML ready, the access manager allows you to use other techniques to enable SSO including:

- Header injection
- Form fill
- Query string parameters

http://www.openiam.com  
sales@openiam.com
OpenIAM also provides implementation of security frameworks such as JAAS and Spring Security. This type of comprehensive strategy allows for applications to be rapidly integrated for SSO.

**FEDERATION**

Federation based SSO is increasingly becoming the preferred method of carrying out SSO. This standards based approach allows applications to be “plugged” into the security environment for SSO with a minimal amount of effort.

- Federation refers to interoperation between entities in different security domains, either in different organizations, or in different tiers in the same organization.
- A trust relationship must exist between the involved entities to federate identity and enable authentication across realms.
- Each domain may rely on different technologies and mechanisms to authenticate and authorize.

As corporations increase their use of cloud applications such as Google Apps, Salesforce.com, and Office365 and the need to seamless SSO into these increases. It’s less then ideal to require users to authenticate into these applications. But it’s a security risk if the enterprise cannot provision and de-provision users from these applications in a timely manner. Imagine a disgruntled employee having access to their corporate systems days after they have been terminated and the damage that can be done.

The OpenIAM Access Manager supports identity federation to address this need. This functionality is integrated with the OpenIAM Identity Manager to provide for an end-to-end solution.

Federation and the overall SSO functionality are integrated into Access Gateway. Since the access gateway also provides authorization, then end result is a solution that goes well beyond the capabilities of pure federation.

**SECURITY TOKEN SERVICE**

A Security Token Service (STS) is a system role defined by the WS-Trust specification. A Web Service Client interacts with the STS to request a security token for use in SOAP messages. In addition, a Web Service Provider interacts with an STS to validate security tokens that arrive in a SOAP message. An STS arbitrates between different security token formats. The token transformation capability defined in WS-Trust provides a standards-based solution to bridge incompatible federation deployments or web services applications.

Web service providers should not be required to support multiple authentication mechanisms even though they have to work with different web service clients. The SAML standard is well recognized and OpenIAM Security Token Service can validate SAML tokens to bridge different web services.
SOA Security

As organizations are tasked with becoming more responsive to market demands, a large number of them are adopting SOA. This architectural philosophy will allow companies to reuse existing services and deliver new business services to customers faster. SOA’s loosely coupled approach that allows accessing applications and services across domains has brought new challenges that complicate security.

OpenIAM believes that an effective SOA security strategy must address the challenges listed below. Further it must meet these challenges:

- Protect distributed services on diverse platforms
- Services cannot implicitly trust each other
- Need for federation due to integration across domains
- Propagate SSO tokens and assertions across SOA
- New security standards to implement
- Solutions must align with existing infrastructure and product selections

OpenIAM Access Manager provides the ability to implement federated relationships as well as protect different layers of the architecture – services, web applications, portals, etc.

In addition to the constructs described earlier, the OpenIAM access manager provides a “Web-service Access Gateway”. This component behaves like the Access Gateway except its primary focus is to protect web services. Call to services are channeled through Web-service Access Gateway where the following occurs:

- Validates that the SOAP request has a valid security token
- Enforces authorization rules, which can be fine grained (ie. Can a person in Role X access the a specific operation on service

By using the Web-service Access Gateway organizations do not need to rely on developers to implement WS-Security on each service. The Web-service Access Gateway allows you to enforce WS-Security in a consistent way across the enterprise.

Conclusion

The security architectures of today’s enterprises face complex demands to provide access for internal and external users to global systems that cannot be satisfied by niche products with limited functionalities or by a proprietary mish-mash of different products with ancient architectures. OpenIAM Access Manager provides an integrated platform with multiple access points and comprehensive functionalities that cover the most demanding environments. It has a modern architecture that facilitates ease of use and integration to enterprise systems. It is a product that has matured through large and challenging deployments.

http://www.openiam.com  sales@openiam.com