What is Identity and Access Management?

Identity and Access Management “IAM” has recently emerged as a critical foundation for realizing the business benefits in terms of cost savings, management control, operational efficiency, and, most importantly, business growth for eCommerce. Enterprises need to manage access to information and applications scattered across internal and external application systems. Moreover, they must provide this access for a growing number of identities, both inside and outside the organization, without compromising security or exposing sensitive information.

IAM comprises of people, processes and products to manage identities and access to resources of an enterprise. Additionally, the enterprise shall have to ensure the correctness of data in order for the IAM Framework to function properly. IAM components can be classified into 4 major categories: authentication, authorization, user management and central user repository (Enterprise Directory). The ultimate goal of IAM Framework is to provide the right people with the right access at the right time – see below diagram “Figure 1 - What is Identity Management”.

![Identity and Access Management Diagram]

**Identity Management**

- **Authentication**
  - Single Sign-On
  - Session Management
  - Password Service
  - Strong Authentication

- **Authorization**
  - Role-based
  - Rule-based
  - Attribute-based
  - Remote Authorization

- **User Management**
  - Delegated Administration
  - User and Role Management
  - Provisioning
  - Password Management
  - Self-service

- **Central User Repository**
  - Directory
  - Data Synchronization
  - Meta-directory
  - Virtual directory

---

*Figure 1 - What is Identity Management*
**Authentication**

This area is comprised of authentication management and session management. Authentication is the module through which a user provides sufficient credentials to gain initial access to an application system or a particular resource. Once a user is authenticated, a session is created and referred during the interaction between the user and the application system until the user logs off or the session is terminated by other means (e.g. timeout). The authentication module usually comes with a password service module when the userid / password authentication method is used. By centrally maintaining the session of a user, the authentication module provides Single Sign-On service so that the user needs not logon again when accesses another application or system governed under the same IAM Framework.

**Authorization**

Authorization is the module that determines whether a user is permitted to access a particular resource. Authorization is performed by checking the resource access request, typically in the form of an URL in web-based application, against authorization policies that are stored in an IAM policy store. Authorization is the core module that implements role-based access control. Moreover, the authorization model could provide complex access controls based on data or information or policies including user attributes, user roles / groups, actions taken, access channels, time, resources requested, external data and business rules.

**User Management**

This area is comprised of user management, password management, role/group management and user/group provisioning. User management module defines the set of administrative functions such as identity creation, propagation, and maintenance of user identity and privileges. One of its components is user life cycle management that enables an enterprise to manage the lifespan of a user account, from the initial stage of provisioning to the final stage of de-provisioning.

Some of the user management functions should be centralized while others should be delegated to end-users. Delegated administration allows an enterprise to directly distribute workload to user departmental units. Delegation can also improve the accuracy of system data by assigning the responsibility of updates to persons closest to the situation and information.

Self-service is another key concept within user management. Through self-profile management service an enterprise benefits from timely update and accurate maintenance of identity data. Another popular self-service function is self-password reset, which significantly alleviates the help desk workload to handle password reset requests.

User management requires an integrated workflow capability to approve some user actions such as user account provisioning and de-provisioning.
Central User Repository

Central User Repository stores and delivers identity information to other services, and provides service to verify credentials submitted from clients. The Central User Repository presents an aggregate or logical view of identities of an enterprise. Directory services adopting LDAPv3 standards have become the dominant technology for Central User Repository. Both Meta-directory and Virtual directory can be used to manage disparate identity data from different user repositories of applications and systems. A meta-directory typically provides an aggregate set of identity data by merging data from different identity sources into a meta-set. Usually it comes with a 2-way data synchronization service to keep the data in sync with other identity sources. A virtual directory delivers a unified LDAP view of consolidated identity information, behind the scene multiple databases containing different sets of users are combined in real time.